IKARUS security software

Benutzerhandbuch

für den

IKARUS security.manager

© 2013 IKARUS Security Software GmbH

1 Inhalt

2 WISSENSWERTES ZU IKARUS ..... - 4 -

3 EINLEITUNG ..... - 5 -

4 IKARUS SECURITY.MANAGER ..... - 6 -

4.1 DER IKARUS SECURITY.MANAGER-SERVER ..... - 7 -
4.2 DIE IKARUS SECURITY.MANAGER-UI ..... - 8 -

5 IKARUS SECURITY.MANAGER INSTALLIEREN ..... - 9 -

5.1 IKARUS SECURITY.MANAGER-SERVER INSTALLIEREN ..... - 10 -
5.1.1 SYSTEMVORAUSSETZUNGEN ..... - 11 -
5.1.2 SQL EXPRESS INSTALLIEREN ..... - 12 -
5.1.3 WILLKOMMEN ..... - 13 -
5.1.4 LIZENZVERTRAG ..... - 14 -
5.1.5 BENUTZEREINSTELLUNGEN ..... - 15 -
5.1.6 NETZWERKEINSTELLUNGEN ..... - 16 -
5.1.7 DATENBANKEINSTELLUNGEN ..... - 17 -
5.1.8 ADMINISTRATOR INFORMATIONEN ..... - 18 -
5.1.9 LDAP-EINSTELLUNGEN ..... - 19 -
5.1.10 BEREITSTELLUNGSEINSTELLUNGEN ..... - 20 -
5.1.11 INSTALLATIONSORDNER AUSWÄHLEN ..... - 21 -
5.1.12 INSTALLATION BESTÄTIGEN ..... - 22 -
5.1.13 LIZENZ HINZUFÜGEN ..... - 23 -
5.1.14 AKTUALISIEREN DES PRODUKTS ..... - 24 -
5.1.15 INSTALLATION ABGESCHLOSSEN ..... - 25 -
5.2 IKARUS SECURITY.MANAGER-UI INSTALLIEREN ..... - 26 -
5.2.1 SYSTEMVORAUSSETZUNGEN ..... - 27 -
5.2.2 WILLKOMMEN ..... - 28 -
5.2.3 LIZENZVERTRAG ..... - 29 -
5.2.4 VERBINDUNG ZUM SERVICE ..... - 30 -
5.2.5 INSTALLATIONSORDNER AUSWÄHLEN ..... - 31 -
5.2.6 INSTALLATION BESTÄTIGEN ..... - 32 -
5.2.7 INSTALLATION ABGESCHLOSSEN ..... - 33 -
5.3 UPGRADE EINER IKARUS SECURITY MANAGER KLEINER VERSION 4.0 ..... - 34 -

6 DIE IKARUS SECURITY.MANAGER-UI ..... - 35 -

6.1 ANMELDUNG ..... - 35 -
6.1.1 PASSWORT FESTLEGEN ..... - 37 -
6.1.2 VERWALTEN MEHRERER IKARUS SECURITY.MANAGER (MANAGEMENT-MODUS) ..... - 39 -
6.1.3 CHANGE MANAGEMENT ..... - 40 -
6.1.4 LIZENZ FESTLEGEN ..... - 41 -
6.1.5 LIZENZVERLETZUNG ..... - 42 -
6.2 DIE BENUTZEROBERFLÄCHE ..... - 44 -
6.2.1 VERZEICHNIS ..... - 45 -
6.2.2 ANSTEHENDE AUFGABEN ..... - 51 -

© 2013 IKARUS Security Software GmbH

6.2.3 VIRENLISTE ..... - 55 -
6.2.4 LOGDATEI ..... - 58 -
6.2.5 CHANGE LOG ..... - 59 -
6.2.6 DIE STARTSEITE ..... - 60 -
6.2.7 EIGENSCHAFTSSEITE ..... - 62 -
6.2.8 SEITE „ALLGEMEIN“ FÜR GRUPPEN ..... - 65 -
6.2.9 SEITE „ALLGEMEIN“ FÜR CLIENTS ..... - 67 -
6.2.10 BENACHRICHTIGUNGSLEISTE ..... - 68 -
6.2.11 DIAGRAMMSEITE ..... - 69 -
6.2.12 GLOBALE STARTSEITE ..... - 71 -
6.2.13 IKARUS ANTI.VIRUS -KONFIGURATIONEN ..... - 73 -
6.2.14 IKARUS SECURITY.MANAGER-EINSTELLUNGEN ..... - 84 -
6.2.15 DIALOG „HOST-EINTRÄGE AUS DER DATENBANK LÖSCHEN“ ..... - 95 -
6.2.16 MANAGEMENT-MODUS ..... - 97 -
6.2.17 INFODIALOG ..... - 107 -
6.2.18 DIE MENÜLEISTE ..... - 108 -
6.2.19 DIE SYMBOLLEISTE ..... - 112 -

7 GETEILTES VERZEICHNIS ..... - 113 -

8 LIZENZINFORMATIONEN ..... - 114 -

8.1 REGISTRIERUNG ..... - 114 -
8.1.1 FENSTERAUFBAU ..... - 114 -
8.2 AKTIVIERUNGSSCHLÜSSEL ..... - 114 -
8.2.1 FENSTERAUFBAU ..... - 115 -

9 SOFTWAREVERTEILUNG ..... - 116 -

9.1 IKARUS ANTI.VIRUS INSTALLIEREN ..... - 117 -
9.2 IKARUS ANTI.VIRUS DEINSTALLIEREN ..... - 119 -

10 KONFIGURATIONSDATEI ..... - 120 -

10.1 DER ABSCHNITT <CONFIG> ..... - 121 -
10.2 DER ABSCHNITT <LDAP> ..... - 122 -

11 ABBILDUNGSVERZEICHNIS ..... - 123 -

12 GLOSSAR ..... - 126 -

© 2013 IKARUS Security Software GmbH

2 Wissenswertes zu IKARUS

Als einer der ersten Anbieter von Antivirensoftware hat IKARUS nicht nur Pionierarbeit auf diesem Gebiet geleistet, sondern ist nach wie vor ein dynamisches und schnell wachsendes Unternehmen. Seit mehr als 25 Jahren vertrauen Anwender dem herausragenden Virenschutz und der exzellenten Content-Sicherheit unter der Marke IKARUS.

Das Entwicklungsteam rekrutiert sich aus UNIX- und Microsoft-Experten sowie früheren Mitarbeitern von Hochschulen und Forschungsinstituten. Dank seiner zahlreichen Kooperationsabkommen und Sondervereinbarungen mit Fachleuten für IT-Sicherheit ist IKARUS in der Lage, aktuellste Informationen in allen Bereichen der Sicherheitssoftware bereitzustellen und schnellste Reaktionen zu gewährleisten.

Unsere Produktpalette reicht vom einfachen aber wirksamen Virenschutz (**IKARUS anti.virus**) über ausgereifte Software für Netzwerke und Gateways (**IKARUS security.manager**, **IKARUS gateway.security**) bis hin zu **IKARUS web.security**, **IKARUS mail.security und IKARUS wifi.security**, einem Managed-Security-Produkt der High-End-Klasse, mit dem Sie Ihr Netzwerk vor Viren schützen, bevor sie zuschlagen können.

© 2013 IKARUS Security Software GmbH

3 Einleitung

Wir möchten Ihnen zu Ihrer Entscheidung zum **IKARUS security.manager** gratulieren und uns für den Kauf bedanken. Mit dieser ebenso einfachen und wie genialen Lösung versorgen Sie die Computer in Ihrem Netzwerk jederzeit mit den aktuellsten Daten für die Viren- und Spamdatenbank und erhalten außerdem stets sofort die neuesten Updates für **IKARUS anti.virus**. Im Wesentlichen werden die Datenbanken und Updates von zentraler Stelle an die Rechner in Ihrem Netzwerk verteilt, um Bandbreite und Datenvolumen – und damit auch Zeit und Kosten für die Administration – einzusparen.

© 2013 IKARUS Security Software GmbH

4 IKARUS security.manager

Der **IKARUS security.manager** dient der Installation, Aktualisierung, Deinstallation und Konfiguration der **IKARUS anti.virus** in Ihrem Netzwerk.

Der **IKARUS security.manager** besteht aus zwei separaten *Anwendungen*: dem **IKARUS security.manager-Server** und der **IKARUS security.manager-UI**. Beide können auf unterschiedlichen Computern und separat voneinander installiert und ausgeführt werden. Dank dieser Trennung können Sie den Schutz Ihres Netzwerks jederzeit und überall kontrollieren und alle Einstellungen auf dem aktuellen Stand halten.

© 2013 IKARUS Security Software GmbH

4.1 Der IKARUS security.manager-Server

Der **IKARUS security.manager-Server** ist das Herzstück des **IKARUS security.manager**. Er übernimmt nicht nur alle anfallenden Aufgaben bei der Datenverteilung und den statistischen Berechnungen, sondern verwaltet auch die Kommunikation zwischen dem **IKARUS security.manager** und den auf den Computern in Ihrem Netzwerk installierten **IKARUS anti.virus.**

Der **IKARUS security.manager-Server** wird als *Dienst* unter einem Windows-Serverbetriebssystem ausgeführt. Alle Einstellungen und Daten, die der **IKARUS security.manager-Server** verarbeitet, werden in einer *MSSQL*-Datenbank gespeichert, die auf dem gleichen Computer wie der **IKARUS security.manager-Server** installiert sein kann, aber nicht muss. Die Kommunikation zwischen dem **IKARUS security.manager** und den **IKARUS anti.virus** in Ihrem Netzwerk erfolgt über *TCP*, wobei standardmäßig Port 9887 ausgewählt ist. Diesen Port können Sie bei Bedarf in der *Konfigurationsdatei* des **IKARUS security.manager-Servers** ändern.

Da der **IKARUS security.manager-Server** Code remote auf den Computern in Ihrem Netzwerk ausführen können muss, benötigt er entsprechende Rechte. Aus diesem Grund empfehlen wir Ihnen dringend, den **IKARUS security.manager-Server*dienst*** mit einem Benutzerkonto zu installieren, das in Ihrer *Domäne* über Administratorrechte verfügt. Auf diese Weise ist sichergestellt, dass der **IKARUS security.manager-Server** die **IKARUS anti.virus** auf Computern innerhalb Ihrer *Domäne* in Ihrem Netzwerk installieren und administrieren kann. Weitere Informationen zu diesem Thema und zur *Administration* von Computern außerhalb Ihrer *Domäne* finden Sie in Kapitel „Softwareverteilung“.

© 2013 IKARUS Security Software GmbH

4.2 Die IKARUS security.manager-UI

Die **IKARUS security.manager-UI** (User Interface, Benutzeroberfläche) stellt eine grafische Oberfläche für die Steuerung des **IKARUS security.manager-Servers** bereit. Sie können die **IKARUS security.manager-UI** auf jedem Computer installieren, über den Sie den **IKARUS security.manager-Server** steuern können möchten. Weitere Informationen zur Struktur und den verschiedenen Dialogfeldern der **IKARUS security.manager-UI** finden Sie im Abschnitt 6.2.
Hinweis: Die UI muss unter einem Administratorkonto gestartet werden, da ein Update der UI auf eine neuere Version andernfalls fehlschlagen könnte.

© 2013 IKARUS Security Software GmbH

5 IKARUS security.manager installieren

In diesem Kapitel werden Sie durch den Installationsprozess für den **IKARUS security.manager** geleitet. Die Einrichtung umfasst zwei getrennte Installationsprozesse: das Setup für den **IKARUS security.manager-Server** und das Setup für die **IKARUS security.manager-UI**. In beiden Setupprozessen wird zunächst überprüft, ob auf dem Zielsystem die für die Ausführung der *Anwendung* erforderlichen Komponenten vorhanden sind. Fehlen solche Komponenten, so werden sie vor Beginn der eigentlichen Installation des IKARUS-Produkts automatisch installiert. Beachten Sie, dass infolge der Installation fehlender erforderlicher Komponenten ein Neustart des Zielcomputers erforderlich sein kann. In einem solchen Fall wird das Setup nach dem erfolgreichen Neustart des Computers automatisch fortgesetzt.

Hinweis: Zur Installation von Server und UI sind Administratorrechte erforderlich. Ist die UAC (User Access Control, Benutzerzugriffssteuerung) aktiviert, dann starten Sie die Installation über die Funktion ***Als Administrator ausführen***.

© 2013 IKARUS Security Software GmbH

5.1 IKARUS security.manager-Server installieren

Zum Starten der Installation des **IKARUS security.manager-Servers** doppelklicken Sie einfach auf die Datei *Setup-ISM(server)_xxxx* (hierbei steht *xxxx* für die Versionsnummer).

Nach der Auswahl der gewünschten Sprache, wird das Setup automatisch gestartet.

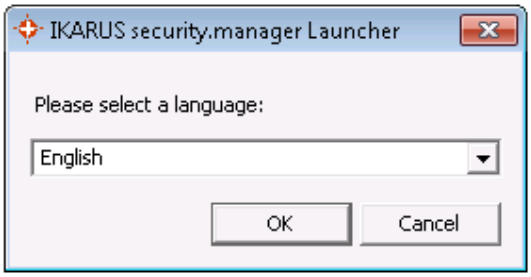


Figure 5-1 UI Installation – Sprachauswahl

© 2013 IKARUS Security Software GmbH

5.1.1 Systemvoraussetzungen

Hardwarevoraussetzungen:

- auf x86-Architektur basierender PC mit einer Prozessorleistung von mind. 2 GHz
- 1 GB RAM
- Bildschirmauflösung: mind. 1024 × 768
- ca. 500 MB verfügbarer Speicherplatz (je nach Anzahl der Logdateien und Größe des Downloadcaches)
- Internetverbindung

Softwareanforderungen:

- Betriebssystem:
  - Client: ab Windows XP SP3
  - Server: ab Windows Server 2003
- *MSSQL* Server ab 2005 (kann auch auf einem anderen als dem Zielcomputer installiert sein)
- *Active Directory* (Microsoft Windows-*Domänen*struktur)

Firewalleinstellungen

Wichtig: Server- und clientseitig werden für die Kommunikation zwischen **IKARUS security.manager** und **IKARUS anti.virus** die Ports 9887 und 9888 verwendet (nach der Erstinstallation).

Diese Ports können geändert werden (siehe *Allgemein*) und müssen als eingehende und ausgehende Regeln auf der Serverfirewall bzw. in der GPO AllePCsFirewall freigegeben werden.

© 2013 IKARUS Security Software GmbH

5.1.2 SQL Express installieren

Der **IKARUS security.manager-Server** benötigt eine *MSSQL*-Datenbank, zum Speichern von Einstellungen, Konfigurationen und *Client*informationen ablegen kann. Diese Datenbank kann auf dem gleichen Computer installiert sein wie der **IKARUS security.manager-Server**, muss es aber nicht.

Sollten Sie, wenn keine lokale Microsoft SQL Version installiert ist, „Vorhandene SQL Installation nutzen“ klicken, müssen Sie einen anderen Rechner angeben, der die entsprechende Datenbank installiert hat. Sollten Sie jedoch eine lokale SQL Instanz benötigen, so kann diese später während dem Setup nicht installiert werden.

Sie können je nach Belieben ein neues "Microsoft SQL Express 2008 R2" oder ein "Microsoft SQL Express 2012" installieren, die beide kostenlos verfügbar sind (Instanz), oder aber eine Version auswählen, die bereits auf dem lokalen Gerät oder auf einem Remote Host vorhanden ist (siehe **Error! Reference source not found.**). Falls Sie eine neue Instanz installieren möchten, müssen Sie diese Software aus dem Internet herunterladen, was bedeutet, dass Sie über eine funktionierende Internet-Verbindung verfügen müssen. Sollte das Herunterladen des gewählten Datenbankmanagementsystems fehlschlagen, dann überprüfen Sie bitte die unter *Netzwerkeinstellungen* gemachten Angaben zum *Proxyserver*, um sicherzustellen, dass Ihre Internetverbindung funktionsfähig ist.

IKARUS security.manager Service Setup
Please verify before you proceed if an existing SQL database is available. You can install it only here a later installation is not possible.
Install SQL Express 2008 R2
Install SQL Express 2012
Use existing database
Install
Close

Abbildung 5-2: Serverinstallation – Installation von SQL Express

© 2013 IKARUS Security Software GmbH

5.1.3 Willkommen

Klicken Sie auf ***Weiter***, um den Lizenzvertrag zu lesen.

IKARUS security.manager Service Setup
Welcome to the IKARUS security.manager Service Setup Wizard
The Setup Wizard will install IKARUS security.manager Service on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel

Abbildung 5-3: Serverinstallation – Willkommen

© 2013 IKARUS Security Software GmbH

5.1.4 Lizenzvertrag

Um die Installation des **IKARUS security.manager-Servers** fortzusetzen, müssen Sie die angezeigten Lizenzbedingungen akzeptieren.

IKARUS security.manager Service Setup
End-User License Agreement
Please read the following license agreement carefully
IKARUS SECURITY SOFTWARE LICENSE AND MAINTENANCE AGREEMENT
Please read this agreement carefully! By installing the delivered software, you agree to be bound by the terms and conditions of the agreement below. If you do not agree to these terms and conditions, terminate the installation procedure and do not use the delivered software any further. Violation of these terms and
I accept the terms in the License Agreement
Print
Back
Next
Cancel

Abbildung 5-4: Serverinstallation – Lizenzvertrag

© 2013 IKARUS Security Software GmbH

5.1.5 Benutzereinstellungen

Der **IKARUS security.manager-Server** wird als *Dienst* installiert. *Dienste* können wahlweise mit lokalen Systemkonten oder einem Benutzerkonto in Ihrer *Domäne* als Anmeldekonto installiert werden. Da der **IKARUS security.manager-Server** bestimmte Rechte benötigt, um eine Binärdatei remote ausführen zu können, wird Ihnen dringend empfohlen, den *Dienst* **IKARUS security.manager Server** unter einem Benutzerkonto zu installieren, dem die Administration der *Domäne* gestattet ist.

Wenn Sie „Service als lokales System starten“ auswählen, müssen Sie zunächst Ihre Benutzerdaten verifizieren, um die Installation fortführen zu können.

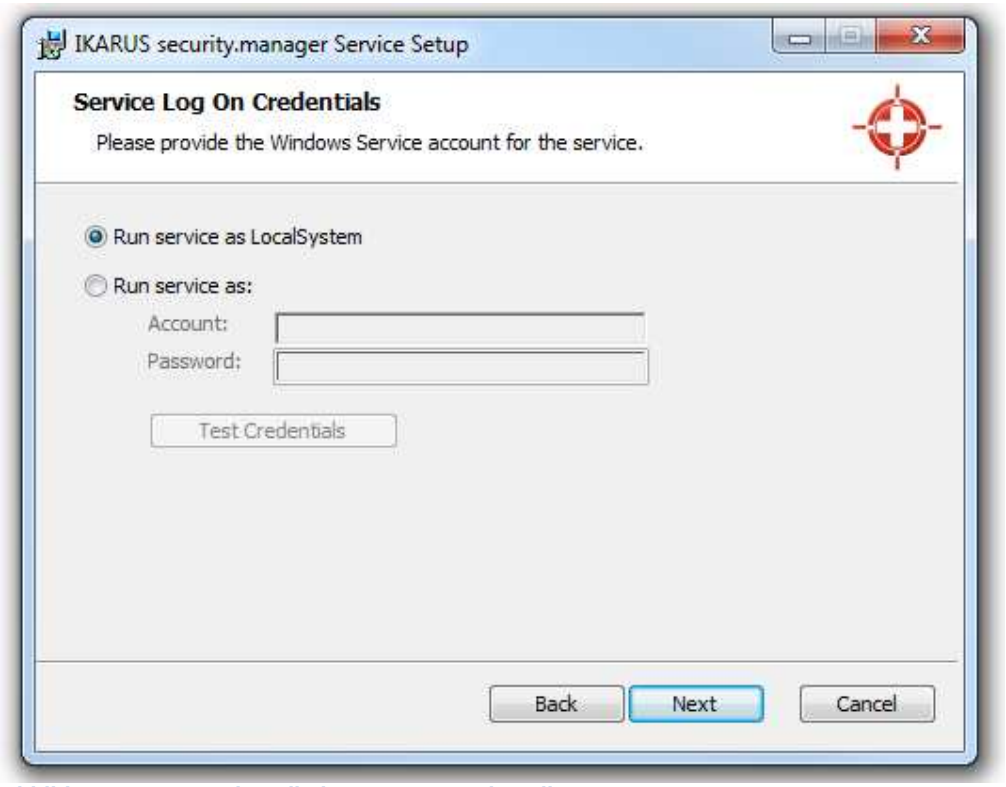


Abbildung 5-5: Serverinstallation – Benutzereinstellungen

Anmerkung: Falls Sie einen **Windows Small Business Server (SBS)** benutzen, verwenden Sie bitte unbedingt das folgende Format für die Anmeldedaten des Domänenbenutzers: **domain\user**. Windows SBS akzeptiert keine Anmeldedaten, welche im Format user@domain eingegeben werden.

© 2013 IKARUS Security Software GmbH

5.1.6 Netzwerkeinstellungen

Wenn Sie einen *Proxyserver* für Ihre Internetverbindung eingerichtet haben, müssen Sie die korrekten Angaben zu Ihrem *Proxyserver* machen, damit der **IKARUS security.manager-Server** auf das Internet zugreifen kann. Es ist zwingend erforderlich, hier die korrekten Informationen anzugeben, um den **IKARUS security.manager** wie vorgesehen verwenden zu können. Bei fehlendem Internetzugang können keinerlei Updates von den IKARUS-Updateservern bezogen werden. **Dies hat zur Folge, dass eine Gefährdung Ihres Netzwerks nicht mehr ausgeschlossen werden kann**.

Abbildung 5-6: Serverinstallation – Netzwerkeinstellungen

© 2013 IKARUS Security Software GmbH

5.1.7 Datenbankeinstellungen

Wenn Sie eine *MSSQL*-Datenbank auf einem anderen Computer angeben möchten, klicken Sie bitte einfach auf **Benutzerdefinierte Verbindung** (siehe **Error! Reference source not found.**) und ersetzen Sie die Zeichenfolge "*SERVER=.*" durch "*SERVER=SERVER_NAME*". Hierbei ist "SERVER_NAME" durch den Servernamen des Zielcomputers zu ersetzen, auf dem die MSSQL-Datenbank eingerichtet ist.

Falls Sie bereits mindestens eine *MSSQL*-Instanz installiert haben, werden Ihnen die installierten Instanzen im Verlauf des Setups zur Auswahl angezeigt.

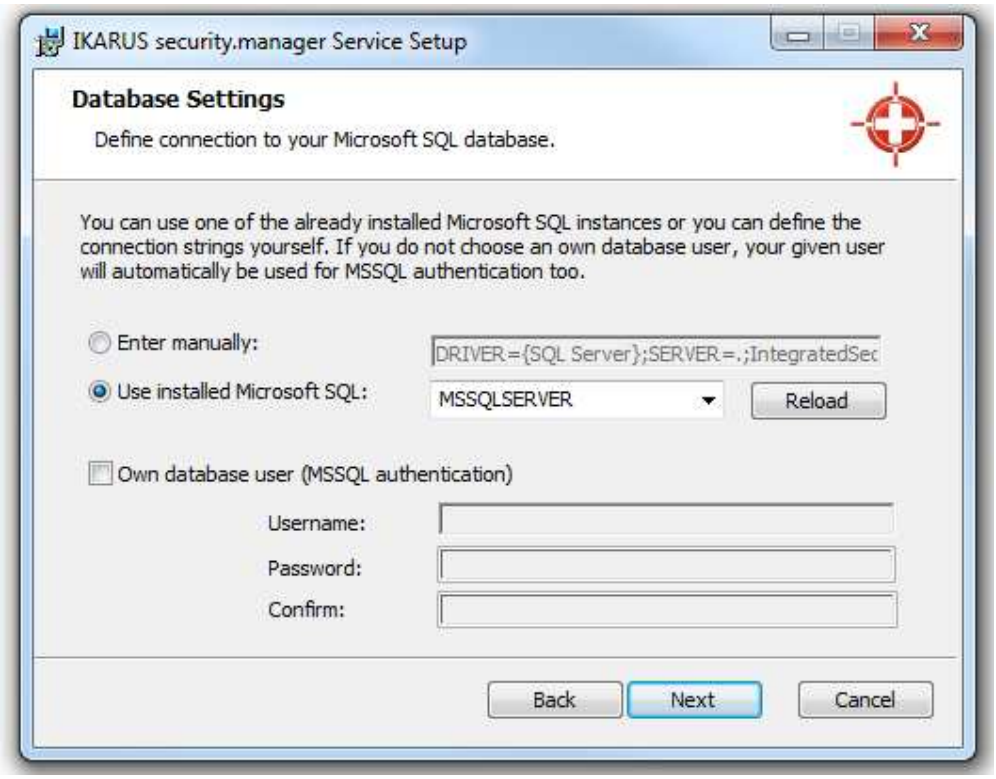

IKARUS security.manager Service Setup
Database Settings
Define connection to your Microsoft SQL database.
You can use one of the already installed Microsoft SQL instances or you can define the connection strings yourself. If you do not choose an own database user, your given user will automatically be used for MSSQL authentication too.
Enter manually:
DRIVER={SQL Server};SERVER=.;IntegratedSec
Use installed Microsoft SQL:
MSSQLSERVER
Reload
Own database user (MSSQL authentication)
Username:
Password:
Confirm:
Back
Next
Cancel

Abbildung 5-7 Server-Installation – Datenbankeinstellungen

© 2013 IKARUS Security Software GmbH

5.1.8 Administrator Informationen

Geben Sie bitte eine valide E-Mailadresse an, damit IKARUS security.manager Service Ihnen in wichtigen Fällen eine Benachrichtigung zukommen lassen kann. Serverport definiert den Port mit dem IKARUS security.manager Service und IKARUS security.manager UI miteinander kommunizieren können. Der Client-Updateport wird benötigt um das instalierte Produkt später korrekt aktualisieren zu können.

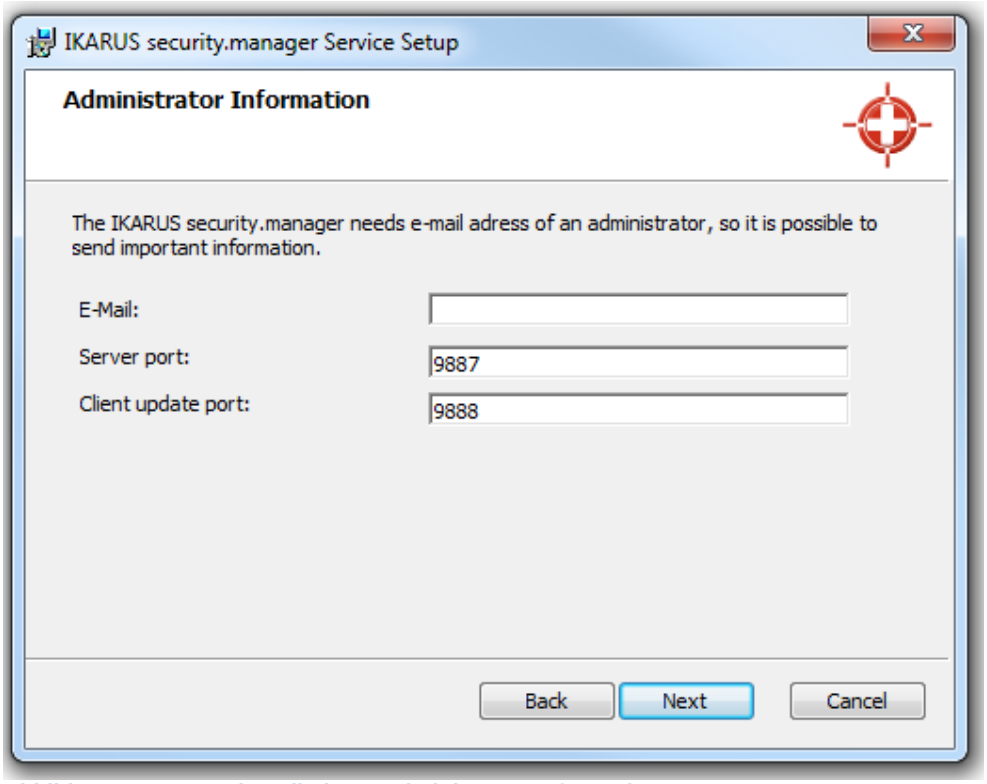


Abbildung 5-8: Serverinstallation – Administrator Informationen

5.1.9 *LDAP*-Einstellungen

Falls das Setup für den **IKARUS security.manager-Server** die erforderlichen Informationen zu Ihrer *LDAP*-Konfiguration nicht automatisch auslesen und bereitstellen kann, können Sie den Servernamen und die Anmeldeinformationen, die vom **IKARUS security.manager-Server** für die Kommunikation mit dem *LDAP*-Server verwendet werden sollen, auch manuell definieren.

Abbildung 5-9: Serverinstallation – LDAP-Einstellungen

© 2013 IKARUS Security Software GmbH

5.1.10 Bereitstellungseinstellungen

Damit die **IKARUS anti.virus** in Ihrem Netzwerk verteilt werden können, benötigt der **IKARUS security.manager-Server** einen Speicherort für die Binärdateien, mit denen die Installation der **IKARUS anti.virus** verwaltet wird. Hierzu müssen Sie (sofern Sie dies nicht bereits getan haben) eine *Netzwerkfreigabe* erstellen, für die alle *Clients*, auf denen sie die **IKARUS anti.virus** installieren möchten, zumindest Leserechte haben. Weitere Informationen zur Bereitstellung der **IKARUS anti.virus** finden Sie in den Abschnitten *„Softwareverteilung“* und *„Geteiltes Verzeichnis*

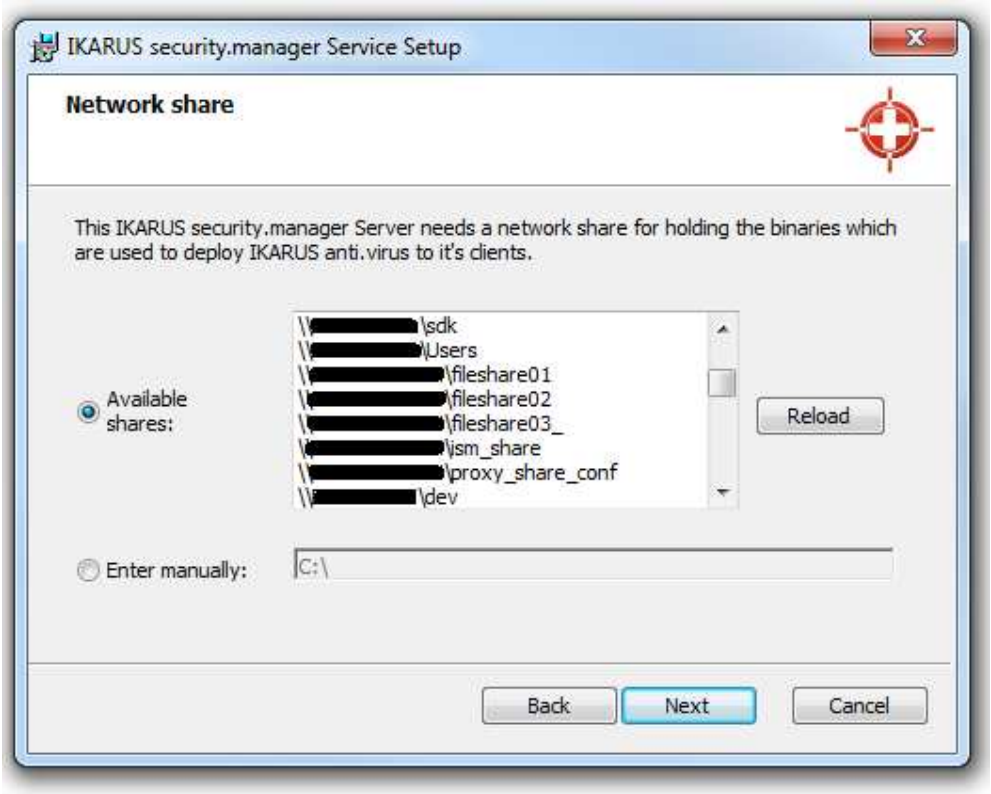


Abbildung 5-10: Serverinstallation – Bereitstellungseinstellungen

© 2013 IKARUS Security Software GmbH

5.1.11 Installationsordner auswählen

Hier können Sie den Zielordner auswählen, in dem die Dateien für den **IKARUS security.manager-Server** installiert werden.

Abbildung 5-11: Serverinstallation – Installationsordner auswählen

© 2013 IKARUS Security Software GmbH

5.1.12 Installation bestätigen

Dies ist der letzte Schritt vor Beginn der eigentlichen Installation der Dateien für den **IKARUS security.manager-Server**. Klicken Sie auf ***Weiter***, um den Kopiervorgang zu starten.

IKARUS security.manager Service Setup
Ready to install IKARUS security.manager Service
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

Abbildung 5-12: Serverinstallation – Installation bestätigen

© 2013 IKARUS Security Software GmbH

5.1.13 Lizenz hinzufügen

Wenn eine Lizenz bereits erworden wurde, kann sie in diesem Dialog geladen werden. Wenn Sie jedoch zuerst eine Lizenz kaufen wollen, klicken Sie auf „Lizenz erwerben“. Spätestens beim Einloggen mit Hilfe von IKARUS security.manager UI werden Sie nochmals nach einer Lizenz gefragt, falls Sie noch keine angegeben haben.

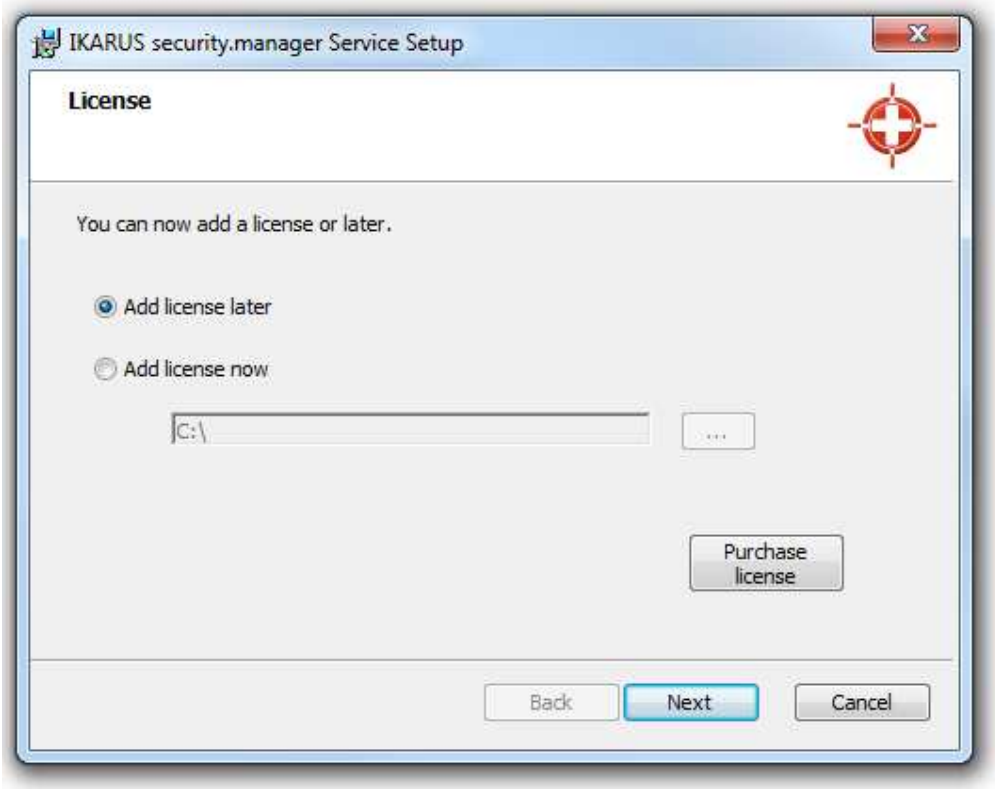


Abbildung 5-13: Server Installation – Lizenz hinzufügen

© 2013 IKARUS Security Software GmbH

5.1.14 Aktualisieren des Produkts

Dies ist der letzte Schritt der Installation. Nachdem Sie auf Weiter geklickt haben, warden zunächst die aktuellen Dateien geladen sofern Sie eine Lizenz angegeben haben. Als letzter Schritt wird IKARUS security.manager Service initialisiert und als Service gestartet.

Figure 5-14 Server Installation – Aktualisieren des Produkts

5.1.15 Installation abgeschlossen

Herzlichen Glückwunsch! Sie haben den **IKARUS security.manager-Server** erfolgreich installiert. Sollte in diesem Fenster ein anderer Text erscheinen, dann wenden Sie sich bitte an die IKARUS-Supporthotline.

Abbildung 5-15: Serverinstallation – Installation abgeschlossen

© 2013 IKARUS Security Software GmbH

5.2 IKARUS security.manager-UI installieren

Zum Starten der Installation der **IKARUS security.manager-UI** doppelklicken Sie einfach auf die Datei *Setup-ISM(UI)_xxxx* (hierbei steht *xxxx* für die Versionsnummer).

Nach der Auswahl der gewünschten Sprache, wird das Setup automatisch gestartet.

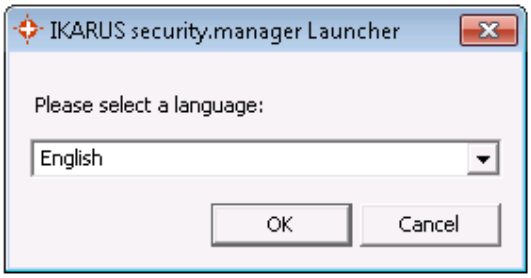


Figure 5-16 UI Installation – Sprachauswahl

© 2013 IKARUS Security Software GmbH

5.2.1 Systemvoraussetzungen

Hardwarevoraussetzungen:

- auf x86-Architektur basierender PC mit einer Prozessorleistung von mind. 2 GHz
- 1 GB RAM
- Bildschirmauflösung: mind. 1024 × 768
- ca. 20 MB verfügbarer Speicherplatz
- LAN-Verbindung

Softwareanforderungen:

- Windows 2003 Server, Windows 2008 Server, Windows 2012 Server (32-Bit- oder 64-Bit-Version)
- Windows XP, Windows Vista, Windows 7, Windows 8 (32-Bit- oder 64-Bit-Version)
- .NET Framework 4.0

© 2013 IKARUS Security Software GmbH

5.2.2 Willkommen

Klicken Sie auf ***Weiter***, um den Lizenzvertrag zu lesen.

IKARUS security.manager UI Setup
Welcome to the IKARUS security.manager UI Setup Wizard
The Setup Wizard will install IKARUS security.manager UI on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel

Abbildung 5-17: UI-Installation – Willkommen

© 2013 IKARUS Security Software GmbH

5.2.3 Lizenzvertrag

Um die Installation der **IKARUS security.manager-UI** fortzusetzen, müssen Sie die angezeigten Lizenzbedingungen akzeptieren.

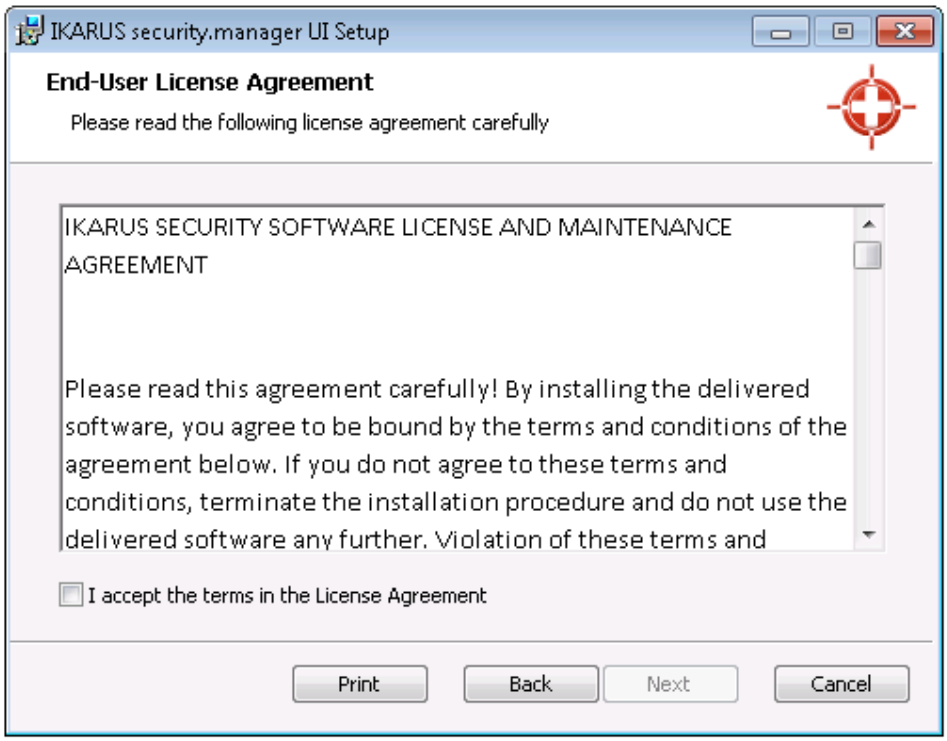

IKARUS security.manager UI Setup
End-User License Agreement
Please read the following license agreement carefully
IKARUS SECURITY SOFTWARE LICENSE AND MAINTENANCE AGREEMENT
Please read this agreement carefully! By installing the delivered software, you agree to be bound by the terms and conditions of the agreement below. If you do not agree to these terms and conditions, terminate the installation procedure and do not use the delivered software any further. Violation of these terms and
I accept the terms in the License Agreement
Print
Back
Next
Cancel

Abbildung 5-18: UI-Installation – Lizenzvertrag

© 2013 IKARUS Security Software GmbH

5.2.4 Verbindung zum Service

In diesem Dialog muss der Port eingegeben warden, mit Hilfe dessen IKARUS security.manager UI und IKARUS.security Service kommunizieren können. Der Standardport ist 9887. Bitte beachten Sie, dass dieser Port nicht durch eine Firewall geblockt werden darf.

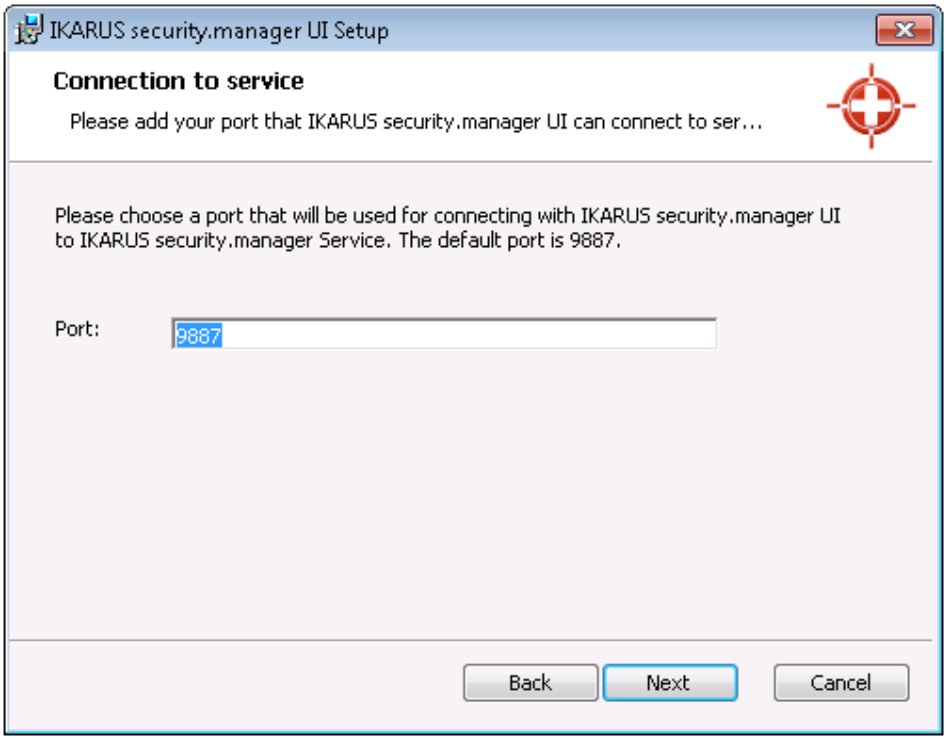

IKARUS security.manager UI Setup
Connection to service
Please add your port that IKARUS security.manager UI can connect to ser...
Please choose a port that will be used for connecting with IKARUS security.manager UI to IKARUS security.manager Service. The default port is 9887.
Port:
9887
Back
Next
Cancel

Figure 5-19 UI Installation – Verbindung zum Service

© 2013 IKARUS Security Software GmbH

5.2.5 Installationsordner auswählen

Hier können Sie den Zielordner auswählen, in dem die Dateien für die **IKARUS security.manager-UI** installiert werden.

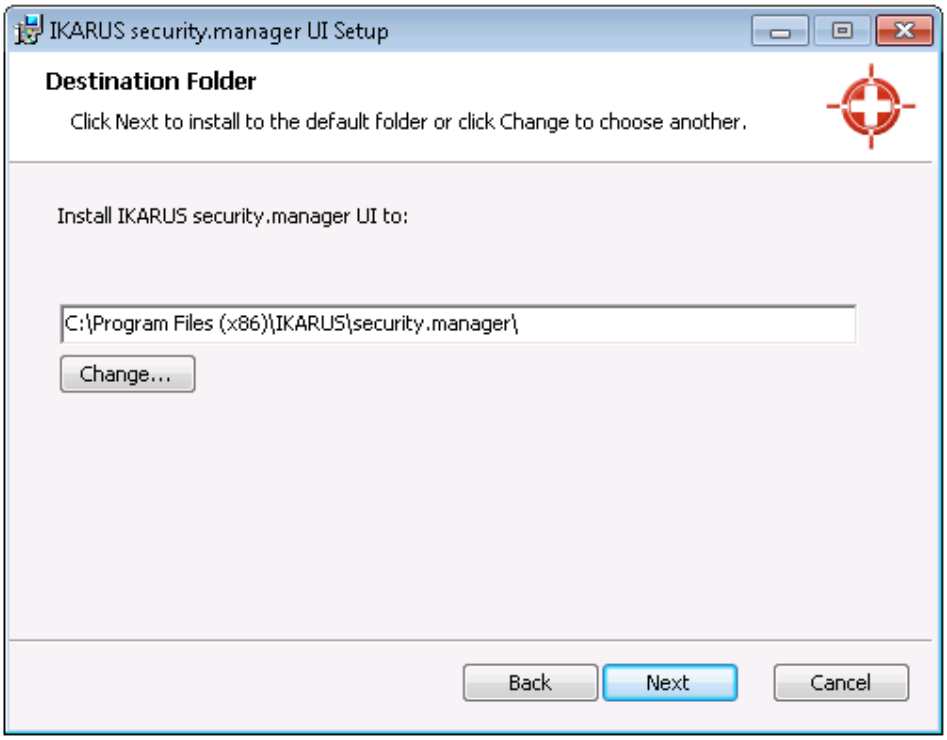


Abbildung 5-20: UI-Installation – Installationsordner auswählen

© 2013 IKARUS Security Software GmbH

5.2.6 Installation bestätigen

Dies ist der letzte Schritt vor Beginn der eigentlichen Installation der Dateien für die **IKARUS security.manager-UI**. Klicken Sie auf ***Weiter***, um den Kopiervorgang zu starten.

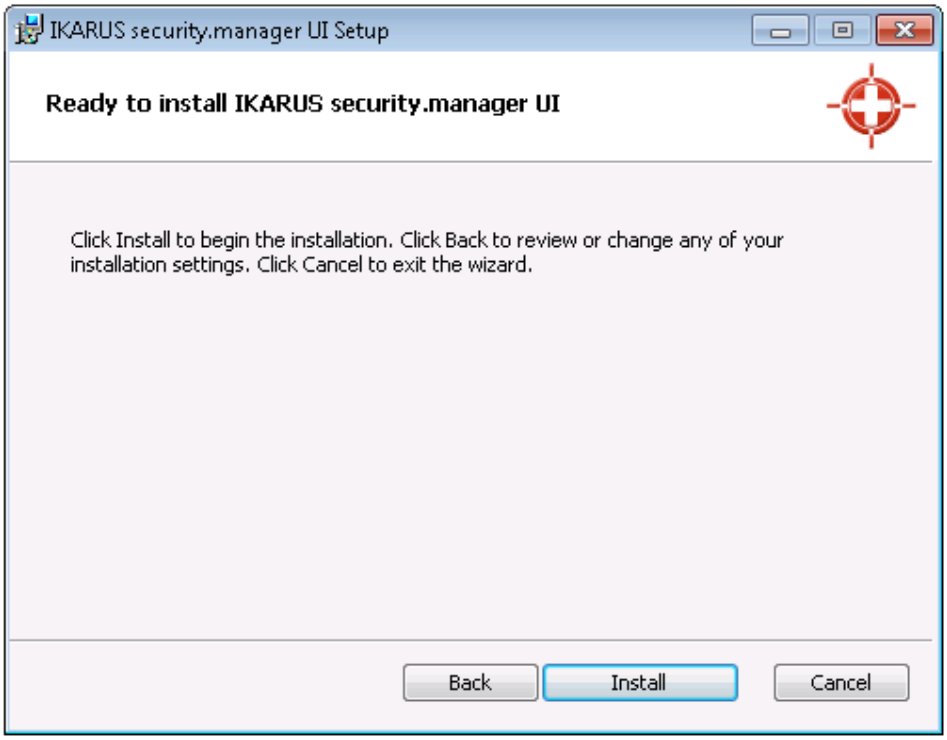

IKARUS security.manager UI Setup
Ready to install IKARUS security.manager UI
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

Abbildung 5-21: UI-Installation – Installation bestätigen

© 2013 IKARUS Security Software GmbH

5.2.7 Installation abgeschlossen

Herzlichen Glückwunsch! Sie haben die **IKARUS security.manager-UI** erfolgreich installiert. Sollte in diesem Fenster ein anderer Text erscheinen, dann wenden Sie sich bitte an die IKARUS-Supporthotline.

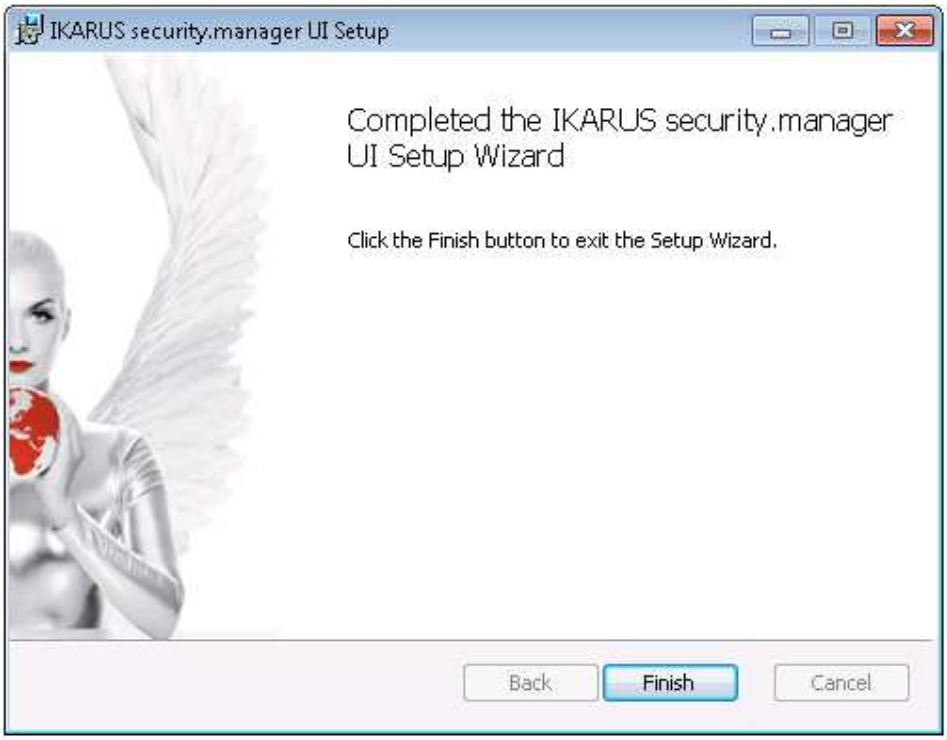


Abbildung 5-22: UI-Installation – Installation abgeschlossen

© 2013 IKARUS Security Software GmbH

5.3 Upgrade einer IKARUS Security Manager kleiner Version 4.0

Das Upgrade eines **IKARUS Security Manager mit einer Version kleiner 4.0** wird, sofern Sie automatische Updates gestattet haben, automatisch durchgeführt. Informationen zu automatischen Updates finden Sie im Abschnitt 6.2.14.4.

Zwar bleibt der Installationspfad unverändert, doch wird die Verzeichnisstruktur während des Upgradevorgangs geändert, und die Binärdateien werden mit neuen Namen versehen. Aus diesem Grund kann es erforderlich sein, ggf. vorhandene Firewallregeln anzupassen.

Nach einem erfolgreichen Upgrade übernimmt die Datenbank die neue Struktur und das neue Layout.
Aufgrund des Upgrades wird eine Sicherungskopie Ihrer alten Datenbank erstellt.
Diese wird im Unterordner *log* Ihres Installationsverzeichnisses unter dem Namen **ISMX_DATABASE_BACKUP.bak** gespeichert.

© 2013 IKARUS Security Software GmbH

6 Die IKARUS security.manager-UI

6.1 Anmeldung

Beim Start der **IKARUS security.manager-UI** erscheint zuerst das Dialogfeld ***Anmeldung*** (Abbildung 5-1), welches zwei verschiedene Modi bietet:

- Einzel-Modus („Login in den Management Modus“ nicht aktiviert)
- Management-Modus („Login in den Management Modus“ aktiviert)

Abbildung 6-1: UI – Anmeldung (Einzel-Modus)

Einzel-Modus
In diesem Modus ist es möglich einen konkreten **IKARUS security.manager** zu verwalten. Daher sind einige Menüpunkte, die im Management-Modus unterstützt werden, nicht aktiv (vgl. Kapitel 6.2.18.5). Um sich zu einem anderem **IKARUS security.manager** zu verbinden, muss der Anmeldevorgang nochmals durchgeführt werden.

Während der Anmeldung werden Sie zur Eingabe Ihrer Anmeldeinformationen und zur Angabe des Servers aufgefordert, mit dem Sie eine Verbindung herstellen möchten (gemeint ist der Servercomputer, auf dem der **IKARUS security.manager-Server** installiert ist). Der *TCP*-Standardport, über den Verbindungen hergestellt werden, ist 9887 für die Kommunikation des **IKARUS security.manager-Servers** mit der **IKARUS security.manager-UI** und 9888 für die Kommunikation zwischen dem **IKARUS security.manager-Server** und **IKARUS anti.virus**-Clients. Sie können diese Ports über den *Oprtionen-Dialog* der **IKARUS security.manager-UI** ändern.

Für Kunden, die nur eine **IKARUS security.manager-Server** Instanz benutzen, bietet sich der Einzel-Modus an.

Management-Modus
Der grundsätzliche Unterschied zum Einzel-Modus ist, dass ein Wechsel zwischen verschiedenen **IKARUS security.manager-Server** ohne weitere Anmeldeovrgänge

© 2013 IKARUS Security Software GmbH

mit Hilfe des Login-Fensters durchgeführt werden kann. Weitere Informationen bezüglich des Wechsels zwischen **IKARUS security.manager-Server** sind in Abschnitt 6.2.1 zu finden. Weiters ändert sich für den Management-Modus auch der Anmeldeprozess. Die Anmeldeinformationen für die einzelnen **IKARUS security.manager-Server** müssen zu einem späteren Zeitpunkt angegeben werden (siehe Abschnitt 6.1.2).

Abbildung 6-2: UI – Anmeldung (Management-Modus)

© 2013 IKARUS Security Software GmbH

6.1.1 Passwort festlegen

Einzel-Modus

Wenn Sie sich zum ersten Mal anmelden, müssen Sie kein Passwort angeben, da Sie noch keines festgelegt haben. Lassen Sie das Feld ***Passwort*** einfach frei, und klicken Sie auf die Schaltfläche ***OK***. Sie werden dann aufgefordert, ein neues Passwort für den angegebenen Benutzer einzugeben.

Abbildung 6-3: UI –Passwort festlegen (Einzel-Modus)

© 2013 IKARUS Security Software GmbH

Management-Modus

Das erforderliche Passwort kann frei gewählt werden und **steht in keiner Abhängigkeit** zu einem **IKARUS security.manager-Server**. Dieses Passwort wird für die Verschlüsselung der Einstellungsdatei für den Management-Modus, welche die gewünschten **IKARUS security.manager** Daten enthält, verwendet.

Abbildung 6-4: UI –Passwort festlegen (Management-Modus)

© 2013 IKARUS Security Software GmbH

6.1.2 Verwalten mehrerer IKARUS security.manager (Management-Modus)

Dieser Schritt is **lediglich im Management-Modus** erforderlich und kann von Kunden, die den Einzel-Modus verwenden, ignoriert werden.

Nachdem ein Passwort für die Einstellungsdatei erstellt wurde, müssen die Daten der gewünschten **IKARUS security.manager-Server** hinzugefügt werden (siehe Abschnitt 6.2.16.1). Weitere Informationen wie das Password für Neuinstallationen gesetzt werden kann, sind ebenfalls aus diesem Abschnitt zu entnehmen.

© 2013 IKARUS Security Software GmbH

6.1.3 Change Management

Einzel-Modus

Wenn die Option ***Nach Request for Change-ID fragen (RfC)*** in den Einstellungen des **IKARUS security.manager-Servers** aktiviert ist (siehe Abschnitt 6.2.14), werden Sie aufgefordert, eine RfC-ID im Anmeldefenster anzugeben (siehe Abbildung 5-3). Wenn die Option ***Nach einem Kommentar fragen bei Log-in Maske*** (siehe Abschnitt 6.2.5) aktiviert ist, werden Sie bei jedem Anmeldeversuch aufgefordert, einen Kommentar einzugeben. Dies ist beispielsweise dann nützlich, wenn Sie Änderungen an den Einstellungen nachverfolgen oder die für die nachfolgende Sitzung geplanten Handlungen erläutern möchten.

Abbildung 6-5: UI – Change Management

Management-Modus

Das Change Management ist für den Management-Modus nicht verfügbar.

© 2013 IKARUS Security Software GmbH

6.1.4 Lizenz festlegen

Wenn Sie im Verlauf des Setups für den **IKARUS security.manager-Server** keine gültige Lizenzdatei angegeben haben, werden Sie nun erneut aufgefordert, eine Lizenzdatei auszuwählen oder die Registrierung unter Angabe eines *Aktivierungsschlüssels* durchzuführen.

© 2013 IKARUS Security Software GmbH

6.1.5 Lizenzverletzung

Sie *verwalten* unter Umständen mehr Clients in Ihrem Netzwerk, als durch Ihre aktuelle Lizenz abgedeckt werden. In diesem Fall liegt eine Lizenzverletzung vor, die ab der **IKARUS security.manager** Version 4.0 erkannt und bearbeitet wird. Sie werden aufgefordert, die überzählige Anzahl Clients aus der *Verwaltung* zu entfernen, damit die durch die aktuelle Lizenz abgedeckte Anzahl Clients nicht mehr überschritten wird.

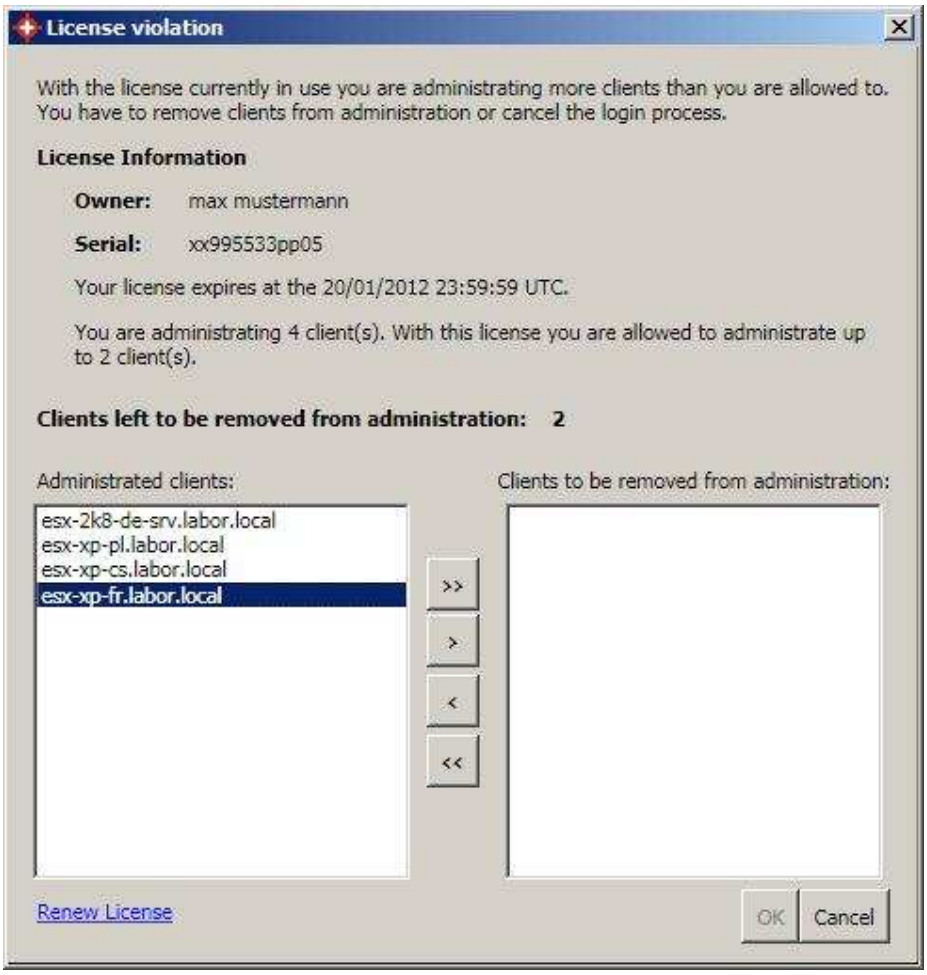

License violation
With the license currently in use you are administrating more clients than you are allowed to.
You have to remove clients from administration or cancel the login process.
License Information
Owner: max mustermann
Serial: xx995533pp05
Your license expires at the 20/01/2012 23:59:59 UTC.
You are administrating 4 client(s). With this license you are allowed to administrate up to 2 client(s).
Clients left to be removed from administration: 2
Administrated clients:
esx-2k8-de-srv.labor.local
esx-xp-pl.labor.local
esx-xp-cs.labor.local
esx-xp-fr.labor.local
Clients to be removed from administration:
>>
>
<
<<
Renew License
OK
Cancel

Abbildung 6-6: UI – Lizenzverletzung

Lizenzinformationen: Hier werden das Ablaufdatum und die genutzte bzw. freie Kapazität Ihrer Lizenz angezeigt.

Clients, die nicht mehr verwaltet werden sollen: Gibt an, wie viele Clients aus der Verwaltung entfernt werden müssen.

Schaltflächen für das Verschieben:

>> Verschiebt alle Clients in die rechte Liste.

> Verschiebt ausgewählte Clients in die rechte Liste.

< Verschiebt ausgewählte Clients in die linke Liste.

© 2013 IKARUS Security Software GmbH

Verschiebt alle Clients in die linke Liste.

Verwaltete Clients: Liste aller verwalteten Clients.

Liste aller Clients, die aus der Verwaltung entfernt werden sollen: Liste aller Clients, die aus der Verwaltung entfernt werden sollen.

Lizenz erneuern: Öffnet das Registrierungsfenster, siehe Abschnitt 7.1.

Mithilfe der Schaltfläche **OK** werden sämtliche Änderungen bestätigt. Diese Schaltfläche ist nur dann aktiviert, wenn Sie die entsprechende Anzahl von Clients auswählen. Sie können diesen Prozess zwar **abbrechen**, können sich jedoch erst dann bei der **IKARUS security.manager**-Benutzeroberfläche anmelden, wenn dieses Problem gelöst ist. Auch wenn Sie den Prozess abbrechen, werden die Clients weiterhin vom **IKARUS security.manager**-Server verwaltet und geschützt.

Für Nachlizenzierungen oder Fragen zu Ihrer erworbenen Lizenz wenden Sie sich bitte an unsere Vertriebs-Abteilung unter*sales@ikarus.at*.

© 2013 IKARUS Security Software GmbH

6.2 Die Benutzeroberfläche

Der Aufbau der **IKARUS security.manager-UI** kann individuell angepasst werden. Jedes Fenster kann an beliebiger Stelle verankert oder schwebend angeordnet werden. Beim Schließen der **IKARUS security.manager-UI** wird die individuelle Anordnung gespeichert.

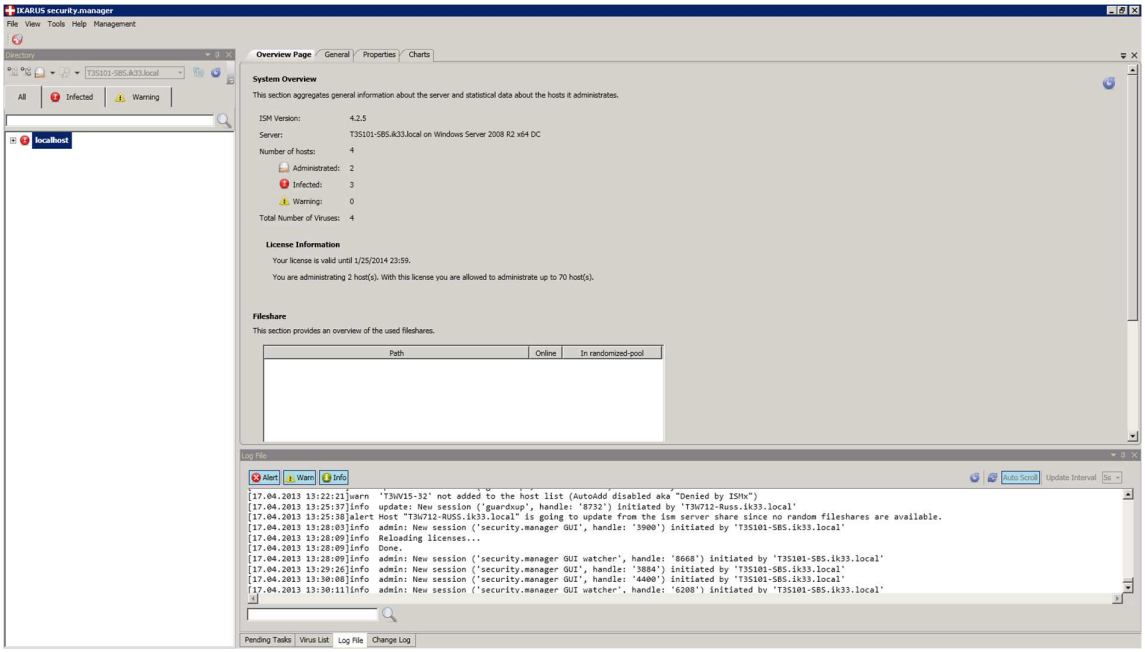

IKARUS security.manager
File View Tools Help Management
Directory
All
Infected
Warning
localhost
Overview Page
General
Properties
Charts
System Overview
This section aggregates general information about the server and statistical data about the hosts it administrates.
ISM Version: 4.2.5
Server: T3S101-SBS.ik33.local on Windows Server 2008 R2 x64 DC
Number of hosts: 4
Administrated: 2
Infected: 3
Warning: 0
Total Number of Viruses: 4
License Information
Your license is valid until 1/25/2014 23:59.
You are administrating 2 host(s). With this license you are allowed to administrate up to 70 host(s).
Fileshare
This section provides an overview of the used fileshares.
Path
Online
In randomized-pool
Log File
Alert
Warn
Info
Auto Scroll
Update Interval
[17.04.2013 13:22:21]warn 'T3WV15-32' not added to the host list (AutoAdd disabled aka "Denied by ISMx")
[17.04.2013 13:25:37]info update: New session ('guardxup', handle: '8732') initiated by 'T3W712-Russ.ik33.local'
[17.04.2013 13:25:38]alert Host "T3W712-RUSS.ik33.local" is going to update from the ism server share since no random fileshares are available.
[17.04.2013 13:28:03]info admin: New session ('security.manager GUI', handle: '3900') initiated by 'T3S101-SBS.ik33.local'
[17.04.2013 13:28:09]info Reloading licenses...
[17.04.2013 13:28:09]info Done.
[17.04.2013 13:28:09]info admin: New session ('security.manager GUI watcher', handle: '8668') initiated by 'T3S101-SBS.ik33.local'
[17.04.2013 13:29:26]info admin: New session ('security.manager GUI', handle: '3884') initiated by 'T3S101-SBS.ik33.local'
[17.04.2013 13:30:08]info admin: New session ('security.manager GUI', handle: '4400') initiated by 'T3S101-SBS.ik33.local'
[17.04.2013 13:30:11]info admin: New session ('security.manager GUI watcher', handle: '6208') initiated by 'T3S101-SBS.ik33.local'
Pending Tasks
Virus List
Log File
Change Log

Abbildung 6-7: UI – Benutzeroberfläche

© 2013 IKARUS Security Software GmbH

6.2.1 Verzeichnis

Das Verzeichnis (Abbildung 5-6) steht im Mittelpunkt aller mit *Clients* verbundenen Bedienschritte. Es enthält die *Clients* Ihres *Active Directory* sowie manuell hinzugefügte *Clients* (d.h. *Clients*, die sich außerhalb Ihrer *Domäne* oder in einer anderen *Domäne* befinden). Alle *Clients* im *Active Directory* werden automatisch mit ihrem jeweiligen *FQDN* aufgelistet. Wir empfehlen **dringend**, für manuell hinzugefügte *Clients* immer den *FQDN* anzugeben, da ein *Client* mit demselben Namen auch in unterschiedlichen *Domänen* vorhanden sein könnte. In diesem Fall gäbe es keine Möglichkeit, zwischen diesen *Clients* zu unterscheiden.

Beachten Sie, dass Sie im Management-Modus zusätzlich die Möglichkeit haben, die **aktuelle Verbindung zu ändern**. Das heißt, sie können sich zu einer anderen **IKARUS Security Manager** Instanz verbinden.

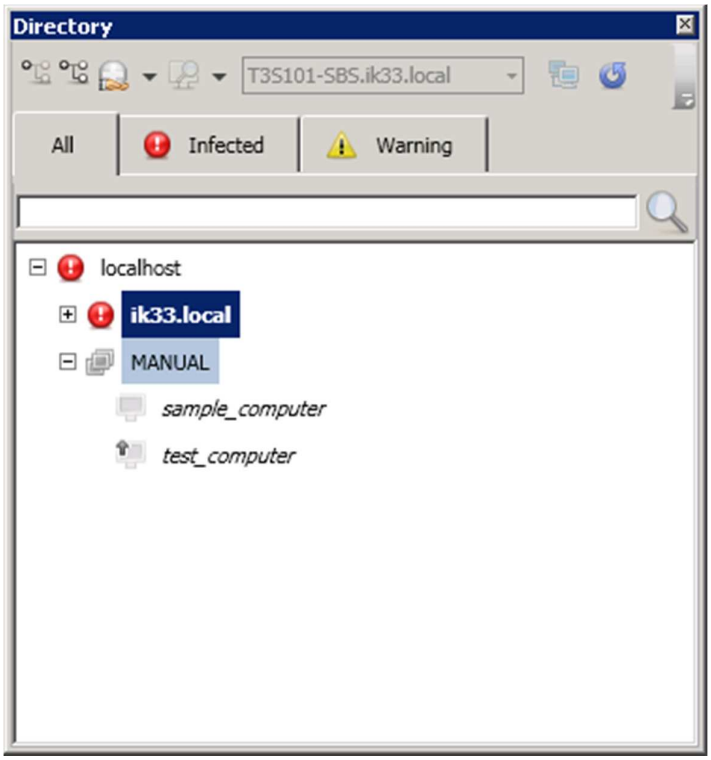


Abbildung 6-8: UI – Verzeichnis (Einzel-Modus)

Das **Verzeichnis**-Fenster besteht aus drei Bereichen. Im oberen Bereich befindet sich die Symbolleiste (siehe Abbildung 6-9) sowie im mittleren Abschnitt die Gruppen-/Clientstruktur. Beim untersten Bereich handelt es sich um den Filterbereich (siehe Abbildung 6-16), in dem in der erwähnten Struktur nach Clients oder Gruppen gesucht werden kann. Die Struktur besitzt auch Filter für Clients mit Warnmeldungen bzw. einer Anzeige infizierter Clients.

© 2013 IKARUS Security Software GmbH

6.2.1.1 *Formatierung*

Knotennamen sind entsprechend ihrem jeweiligen Status wie folgt formatiert:

Normal: Dieser Client ist online.
Kursiv: Dieser Client ist offline.
Fett: Dieser Knoten ist ausgewählt.

6.2.1.2 *Fensteraufbau*

Das *Verzeichnis* ist in die folgenden drei Bereiche unterteilt:

6.2.1.2.1 Symbolleiste:

Abbildung 6-9 UI - Verzeichnissymbolleiste

Die Symbole besitzen von links nach rechts die folgende Bedeutung:

a. Sämtliche Gruppenknoten ausblenden.
b. Sämtliche Gruppenknoten einblenden.
c. Öffnet das Kontextmenü für den aktuell ausgewählten Client (siehe "Kontextmenü" in diesem Abschnitt).
d. Scanoptionen, siehe nächste Abbildung.
e. Auswahl der IKARUS Security Manager Instanz (siehe „Wechseln der aktuellen IKARUS Security Manager Instanz“ in diesem Abschnitt)
f. Stellt die Verbindung erneut her (siehe „Verbindung neu herstellen“ in diesem Abschnitt)
g. Aktualisiert das Verzeichnis

Die Scanoptionen: Abbildung 6-10 zeigt mögliche Scanoptionen.

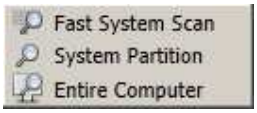


Abbildung 6-10 Die Scanoptionen

- **Schneller Systemscan:** Windows-Verzeichnis und aktive Prozesse scannen (nur auf aktuell ausgewähltem Client).
- **Systempartition:** Systempartition scannen (nur auf aktuell ausgewähltem Client).
- **Ganzer Computer:** Gesamtes System scannen (nur auf aktuell ausgewähltem Client).

Das Kontextmenü: Abbildung 6-11 zeigt sämtliche Einstellungsoptionen des Kontextmenüs, die nach Rechtsklicken erscheinen.

© 2013 IKARUS Security Software GmbH

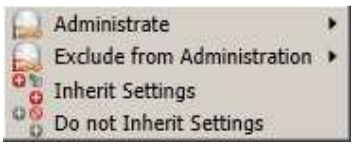


Abbildung 6-11 Das Kontextmenü für clientbezogene Aktionen

Verwalten/von Verwaltung ausnehmen: Dieses Kontextmenü ist außerdem in weitere Einstellungsoptionen unterteilt (siehe Abbildung 6-12):

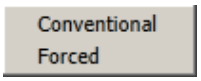


Abbildung 6-12 Optionen für die Verwaltung bzw. das Ausnehmen von der Verwaltung

- **Verwaltung aktivieren/deaktivieren:** Updates und Systemschutz ein-/ausschalten.
- **Verwaltung aktivieren/ deaktivieren erzwingen:** Verwaltung durch anderen **IKARUS security.manager** wird ignoriert.

Einstellungen erben/nicht erben: Einstellungen werden vom übergeordneten Knoten (nicht) übernommen.

Wechseln der aktuellen IKARUS Security Manager Instanz: Das Kernfeature der neuen Version des IKARUS Security Managers ist, dass man mit derselben Oberfläche mehrere IKARUS Security Manger Instanzen verwalten kann. Sie können über die Auswahlbox auswählen, zu welcher Instanz Sie sich verbinden wollen. Dieses Steuerelement ist nur im Multi-Instanz Modus aktiviert – im Einzel-Instanz Modus wird die Verbindung nur zu jener IKARUS Security Manager Instanz aufgebaut, deren Daten Sie im Login-Screen angegeben haben.

Verbindung neu herstellen: Dieser Button ist aktiviert, wenn der Verbindungsaufbau zur in der Auswahlbox gewählten IKARUS Security Manager Instanz fehlgeschlagen ist. Schuld an eine fehlgeschlagene Verbindung können falsche Verbindungsdaten sein. Sie können diese gegebenenfalls im Optionen-Menü (siehe 5.2.16.1) bearbeiten. Ein Klick auf den Button bewirkt einen erneuten Verbindungsaufbau.

© 2013 IKARUS Security Software GmbH

6.2.1.2.2 Gruppen-/Clientstruktur:

Der in der **Gruppen-/Clientstruktur** angezeigte Hauptknoten ist stets der erste Knoten und trägt die Bezeichnung "Alle". Dieser sowie alle anderen Knoten, denen dasselbe Symbol vorangestellt ist, sind Gruppenknoten.

Knoten mit einem vorangestellten Computerschirm sind Clientknoten (z.B. Knoten mit der Bezeichnung "manueller Computer").

Abbildung 6-13 Die Gruppen/Clientstruktur

Das Kontextmenü wird durch Rechtsklicken auf ein Element geöffnet. In der Abbildung unten sind alle möglichen Optionen des Kontextmenüs zu sehen, welche jedoch nicht immer verfügbar sind. Die ersten vier Optionen (**Gruppe hinzufügen, Computer hinzufügen, Löschen** und **Umbenennen**) stehen nur für manuell hinzugefügte Gruppen/Clients zur Verfügung. Die restlichen Einträge stehen immer zur Verfügung, sobald eine Gruppe selektiert wird. Ist ein Client selektiert, so werden nur die möglichen Aktionen dargestellt (z.B. wenn ein Host die Einstellungen erbt, so ist nur der Menüpunkt „Die Einstellungen nicht vererben“ sichtbar). Bitte beachten Sie, dass die Ermittlung Daten der Gruppen/Clients nach einer Aktualisierung einige Zeit benötigen, um korrekt dargestellt zu werden.

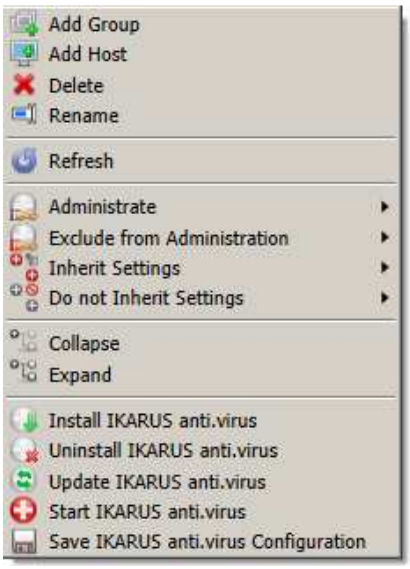


Abbildung 6-14 Das Kontextmenü für eine Gruppe bzw. einen Client

© 2013 IKARUS Security Software GmbH

6.2.1.2.3 *Kontext Menü ‚Werkzeuge“*:

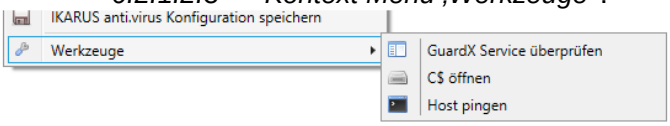


Abbildung 6-15 Kontext Menü ‚Werkzeuge‘

Das Kontext Menü „Tools“ bietet Funktionen an, um die Verbindung zu einem Klient zu überprüfen:

- **GuardX Service überprüfen**: Versucht den GuardX Service am ausgewählten Klient zu erreichen.
- **C$ öffnen**: Öffnet C$ des gewählten Host. Benötigt unter Umständen die Benutzerdaten des Hosts.
- **Host pingen**: Sendet ein ping-Kommando an den Host und zeigt das Ergebnis an.

6.2.1.2.4 *Filterbereich:*

Abbildung 6-16 UI – Verzeichnisfilter

Der Filterbereich des Verzeichnisses ermöglicht das Festlegen eines Filters innerhalb eines Textfelds (ohne Unterscheidung nach Groß-/Kleinbuchstaben). Es werden nur Knoten angezeigt, die den Filterkriterien entsprechen. Das nächste Element, welches den Filterkriterien entspricht, wird mithilfe des Vergrößerungsglases angezeigt.

Registerkarten mit vordefinierten Filtern (siehe Abbildung oben):

- **Alle** (aktiv): Überblick über alle Clients, die sich in Ihrem Verzeichnis befinden, sowie über alle manuelle hinzugefügten Clients.
- **Infiziert** (inaktiv): Überblick über alle infizierten Clients.
- **Warnung** (inaktiv): Überblick über alle veralteten Clients, also solche mit einer Viren- oder Spamdatenbank (bei aktivierter Spamerkennung) und einem anti.virus -Update, das älter als 2 Wochen ist. Clients, die verwaltet werden und online sind, aber IKARUS anti.virus nicht ausführen oder vom IKARUS security.manager nicht erreicht werden, sind ebenfalls aufgeführt.

© 2013 IKARUS Security Software GmbH

6.2.1.3 *Symbole*

Die Symbole der Knoten im *Verzeichnis* bieten einen schnellen Überblick über den Status der einzelnen Knoten.

Dieser Knoten ist eine **Gruppe**.

Dieser Client ist **offline**.

Dieser Client ist **online**; **IKARUS anti.virus** ist darauf **nicht** installiert.

Dieser Client ist **online** und wird **verwaltet; IKARUS anti.virus** ist darauf installiert.

Dieser Client ist **online** und wird **nicht verwaltet; IKARUS anti.virus** ist darauf installiert.

(Eingeblendet) Dieser Knoten **erbt die Einstellungen des übergeordneten Elements**.

(Eingeblendet). Dieser Knoten oder ein ihm untergeordnetes Element **ist infiziert**.

(Eingeblendet) Dieser Knoten oder ein ihm untergeordnetes Element **ist veraltet oder wird verwaltet, ist jedoch nicht erreichbar.**

6.2.1.4 *Manuelle Gruppe*

Die manuelle Gruppe (als **MANUAL** im *Verzeichnis* aufgeführt) ist der unterste Gruppenknoten im Stammknoten (**Alle**) des *Verzeichnisses*. Dieser Gruppe können Sie hier Computer hinzufügen, die Mitglied einer anderen *Domäne* sind oder aus überhaupt keiner *Domäne* stammen. Sie können Knoten (*Clients* und Gruppen) beliebig hinzufügen, umbenennen, entfernen und verschieben.

6.2.1.5 *Mehrfachauswahl*

Mehrere Knoten können **ausgewählt** werden, indem Sie sie **bei gedrückter Strg-Taste anklicken**. Stellen Sie sich die Mehrfachauswahl als **temporären Gruppenknoten** vor, der nicht mehr vorhanden ist, sobald Sie die Mehrfachauswahl (beispielsweise durch gezielte Auswahl eines einzelnen Elements) aufheben. **Aktionen und Ansichten, die für Gruppenknoten verfügbar sind**, stehen gleichermaßen **für eine temporäre Gruppe zur Verfügung**.

6.2.1.6 *Gruppen verwalten*

Wenn Sie eine Gruppe verwalten, "erben" alle Unterelemente (Clients und Untergruppen) von dieser Gruppe, und binäre Updates werden automatisch für jeden Client zugelassen.
Alle Clients innerhalb der Gruppe, auf denen die **IKARUS anti.virus** installiert sind, werden durch den **IKARUS security.manager** verwaltet

© 2013 IKARUS Security Software GmbH

6.2.2 Anstehende Aufgaben

Aktionen wie die Installation von **IKARUS anti.virus** oder das *Verwalten bzw. das Beenden der Verwaltung* von Clients werden als Aufgaben auf dem **IKARUS security.manager-Server** abgelegt. Aufgaben sind sitzungsbezogen - verarbeitete Aufgaben gehen verloren, wenn Sie Ihre aktuelle Sitzung in der **IKARUS security.manager-UI** beenden, während nicht erledigte Aufgaben weiterhin verfügbar bleiben. Im Fenster **Anstehende Aufgaben** (Abbildung 6-17) werden alle vorhandenen Aufgaben aufgelistet. Dies umfasst sowohl *client*spezifische als auch die gesamte *Verzeichnis*struktur betreffende Aufgaben mit ihrem jeweiligen Status, dem Ergebnis und der Resolve Time. Unter der Resolve Time ist das Datum zu verstehen, an dem der Aufgabenstatus erneut ausgewertet wird. Je nach Aufgabenstatus wird dann eine Aktion ausgeführt, um die Aufgabe zu erledigen.

Bitte beachten Sie, dass der nächste festgelegte Zeitpunkt veraltet sein kann, wenn die automatische Aktualisierung ausgeschaltet ist oder das Aktualisierungsintervall verlängert wurde. Der Zeitstempel ist daher nur so aktuell wie der letzte Aktualisierungszeitpunkt!

6.2.2.1 *Fensteraufbau*

Symbolleiste oben auf dem Fenster
Die Symbole besitzen von links nach rechts die folgende Bedeutung (siehe Abbildung 6-17):

a. **Anstehen**: Blendet anstehende Aufgaben ein oder aus.
b. **Aktiv**: Blendet aktive Aufgaben ein oder aus.
c. **Wartend**: Blendet wartende Aufgaben ein oder aus
d. **Verarbeitet**: Blendet verarbeitete Aufgaben ein oder aus.
e. **Clientspezifisch**: Zeigt, falls aktiv, die Aufgaben des aktuell im Verzeichnis ausgewählten Knotens, ansonsten sämtliche Aufgaben.
f. **Aktualisieren**: Ruft eine aktualisierte Aufgabenliste ab.
g. **Automatisch Aktualisieren**: Ruft in benutzerdefinierten Abständen eine aktualisierte Aufgabenliste ab.
h. **Update-Intervall**: Bestimmt den zeitlichen Abstand, in dem die Aufgabenliste aktualisiert werden soll.

Liste der anstehenden Aufgaben
In der **Liste der anstehenden Aufgaben** werden sämtliche auf dem **IKARUS security.manager**-Server vorhandene Aufgaben mit ihrem jeweiligen aktuellen Status nach erfolgtem Update vom Server. Aufgaben, die neu gestartet wurden, werden in der Aufgabenliste als Unteraufgabe dargestellt. Bei diesen Aufgaben wird ihr jeweiliger Status ersichtlich (siehe Abschnitt 6.2.2.2). Durch Doppelklicken auf eine Aufgabe wird die dazugehörige Detailansicht aufgerufen (siehe Abschnitt 6.2.2.3).

Nächste geplante Resolve Time zeigt Datum und Uhrzeit an, zu der alle Aufgaben erneut gestartet werden und zu welcher der Server versuchen wird, diese zu lösen.

© 2013 IKARUS Security Software GmbH

Das Kontextmenü für anstehende Aufgaben

Das Kontextmenü wird durch einen Rechtsklick auf eine Aufgabe in der Liste der anstehenden Aufgaben geöffnet. Im Kontextmenü stehen folgende Aktionen zur Auswahl:

- **Erzwingen**: Erzwingt die Fertigstellung der Aufgabe.
- **Stopp**: Beendet die Fertigstellung der Aufgabe.
- **Alles neu starten:** Startet alle Unteraufgaben neu.
- **Neustart nicht vollständig:** Startet nur unvollständige Unteraufgaben neu.
- **Details**: Öffnet die Detailansicht der Aufgabe, siehe Abschnitt 6.2.2.3.

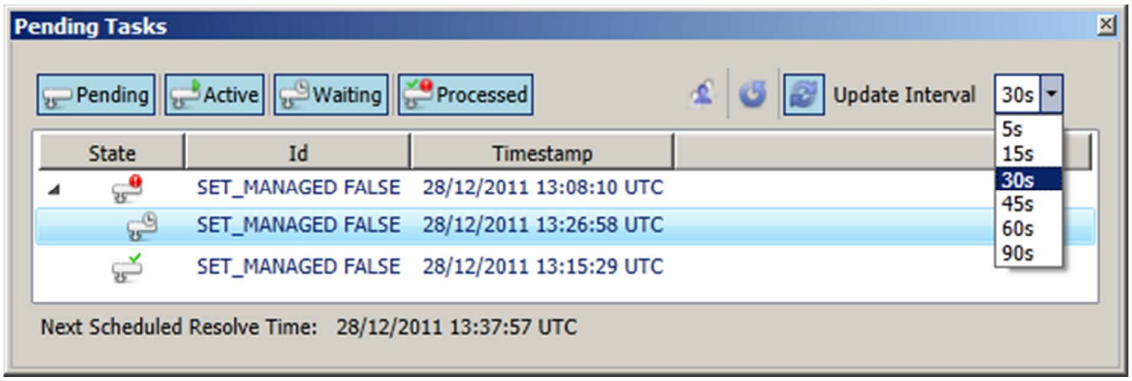


Abbildung 6-17: UI – Anstehende Aufgaben

© 2013 IKARUS Security Software GmbH

6.2.2.2 *Aufgabenzustände*

Symbol	Zustand	Ursache	Aktion zur Behebung
	Aktiv	Die Aktion wird gegenwärtig ausgeführt.	Nur der Aufgabenzustand wird neu ausgewertet.
	Anstehend	Die Aktion wurde noch nicht verarbeitet.	Die Aufgabe wird noch bearbeitet.
	Wartend	Die Aktion wurde mindestens einmal gestartet, aber der oder die Zielclients waren nicht erreichbar.	Es wird weithin versucht, die Zielclients zu erreichen
	Verarbeitet	Die Aktion wurde erfolgreich verarbeitet.	Nur der Aufgabenzustand wird neu ausgewertet.
	Nicht verarbeitet	Die Aktion wurde nicht bearbeitet, weil der Benutzer die Aktion abgebrochen hat.	Nur der Aufgabenzustand wird neu ausgewertet.
	Verarbeitung mit Fehlern	Die Aktion wurde verarbeitet, doch während der Verarbeitung ist ein Fehler aufgetreten.	Nur der Aufgabenzustand wird neu ausgewertet.

6.2.2.3 *Aufgabendetails*

Symbolleiste

- **Anzahl der Hosts**: Zeigt an, wie viele Hosts bei dieser Aufgabe bearbeitet werden.
- **Aktualisieren**: Ruft eine aktualisierte Host- und Aufgabenliste auf.
- **Automatisch aktualisieren**: Ruft in vom Benutzer festgelegten Abständen selbsttätig eine aktualisierte Hostliste auf.
- **Update-Intervall**:. Bestimmt den zeitlichen Abstand, in dem die Hostliste aktualisiert werden soll.

Hostliste

In der ersten Spalte wird der **Hostzustand**, d.h. der Status des Zielhosts, dargestellt (siehe Abschnitt 6.2.1.3). Der **Hostname** des Zielhosts wird in der zweiten Spalte angezeigt, während das **Resultat** der betreffenden Aktion aus der letzten Spalte ersichtlich ist.

© 2013 IKARUS Security Software GmbH

Kontextmenü
Das Kontextmenü wird durch einen Rechtsklick auf eine Eintragung in der Hostliste geöffnet. Die folgenden beiden Aktionen stehen zur Auswahl:

- **Erzwingen**: Erzwingt die Fertigstellung der Aufgabe auf diesem Host.
- **Abbrechen**: Bricht die Fertigstellung der Aufgabe auf diesem Host ab.

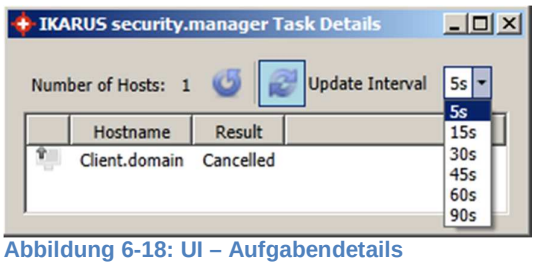


Abbildung 6-18: UI – Aufgabendetails

© 2013 IKARUS Security Software GmbH

6.2.3 Virenliste

Im Fenster Virenliste (siehe Abbildung 5-16) können Sie in Ihrem Netzwerk vorhandene Infektionen näher untersuchen. Sie können wahlweise alle gefundenen Infektionen oder aber nur diejenigen auflisten, die auf dem aktuell ausgewählten Knoten im *Verzeichnis* vorhanden sind.

Mit Hilfe von „Malware“ und „PUA“ (potentiell ungewollte Anwendung) ist es möglich die Virenliste so zu sortieren, um nur die entsprechenden Virenbefunde anzuzeigen.

6.2.3.1 *Fensteraufbau*

Links im **Informationsbereich** können Sie im oberen Drittel des Virenlistenfensters allgemeine Angaben zur Virenliste sehen. Diese Informationen lassen sich mithilfe der Umschaltfläche **Hostspezifisch** reduzieren. Bei erfolgter Aktivierung dieser Umschaltfläche werden die Infektionen aller Clients angezeigt, ansonsten nur die Infektionen jener Knoten, die aktuell im Verzeichnis ausgewählt sind (siehe Abschnitt 6.2.1).

In diesem Bereich wird die **Anzahl der Viren** dargestellt, die in der Liste enthalten sind.

Virenliste
Die Virenliste besteht aus folgenden Informationsspalten:

- **Aktiv:** Diese Spalte scheint nicht mehr in der Virenliste auf und wurde nur vorübergehende in der Version 4.0 des I**KARUS security.manager** dargestellt. Der Begriff "inaktiver Virus" bedeutet, dass solche Viren auf Hosts aufgefunden wurden, welche nicht vom I**KARUS security.manager** verwaltet werden.
- **Hostzustand:** Gibt den Status des Client an, siehe Abschnitt 6.2.1.3.
- **Hostname:** Zeigt den Clientnamen an.
- **Typ:** Zeigt den Typ (Malware oder potentiell ungewollte Anwendung) der Infektion an.
- **Datum:** Datum, an dem die Infektion erkannt wurde.
- **Dateiname:** Name der infizierten Datei.
- **Pfad:** Das Verzeichnis, in welchem die Infektion entdeckt wurde.
- **Virenbeschreibung:** Die Bezeichnung der jeweiligen Infektion. Durch Klicken kann der Virenlexikoneintrag für die betreffende Infektion geöffnet werden.

Durch einen Rechtsklick auf einen Virus in der Liste wird das Kontextmenü geöffnet. Im Kontextmenü stehen folgende Aktionen zur Auswahl:

- **Virenlexikon:** Öffnet den Virenlexikoneintrag für die betreffende Infektion
- **Details:** Öffnet die Detailansicht für die Infektion, siehe Abschnitt 6.2.3.2.
- **An IKARUS Virus Lab senden:** Schickt die Infektion zur Analyse an IKARUS.

Ist die Hostspezifische Ansicht aktiv, sind zusätzlich folgende Optionen verfügbar:

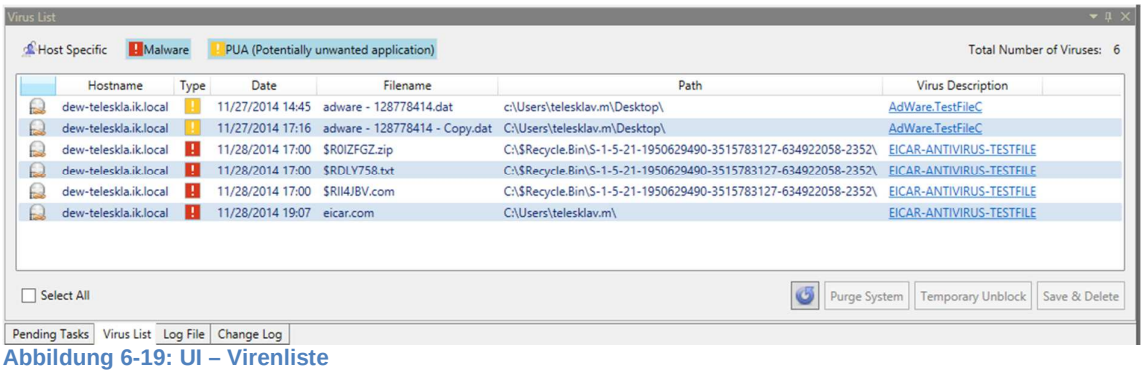
- **Vorrübergehend entsperren**: Infizierte Datei wird vorrübergehend freigegeben.
- **Sichern & Löschen**: Infizierte Datei wird vom Client gelöscht.

© 2013 IKARUS Security Software GmbH

- **Virus ignorieren**: Virus wird aus der Virenliste entfernt, nicht aber vom Client gelöscht. Wenn der Client das nächste Mal seine Virenliste an den **IKARUS security.manager** sendet, taucht der Virus wieder auf.

Aktionsbereich
Im Aktionenbereich unten im Fenster stehen mehrere Funktionen zur Verfügung, die auch in IKARUS anti.virus angeboten werden.

- **Alle auswählen:** Alle Einträge auswählen bzw. nicht auswählen.
- **Schaltfläche "Aktualisieren":** Virenliste aktualisieren
- **System reinigen:** Löscht die in der Liste ausgewählten Infektionen.
- **Vorübergehend entsperren:** Entfernt die Datei aus der Quarantäne.
- **Speichern & Löschen:** Erstellt eine Sicherungskopie der infizierten Datei und löscht das Original.


Virus List
Host Specific
Malware
PUA (Potentially unwanted application)
Total Number of Viruses: 6
Hostname Type Date Filename Path Virus Description
dew-teleskla.ik.local 11/27/2014 14:45 adware - 128778414.dat c:\Users\telesklav.m\Desktop\ AdWare.TestFileC
dew-teleskla.ik.local 11/27/2014 17:16 adware - 128778414 - Copy.dat C:\Users\telesklav.m\Desktop\ AdWare.TestFileC
dew-teleskla.ik.local 11/28/2014 17:00 $R0IZFGZ.zip C:\$Recycle.Bin\S-1-5-21-1950629490-3515783127-634922058-2352\ EICAR-ANTIVIRUS-TESTFILE
dew-teleskla.ik.local 11/28/2014 17:00 $RDLY758.txt C:\$Recycle.Bin\S-1-5-21-1950629490-3515783127-634922058-2352\ EICAR-ANTIVIRUS-TESTFILE
dew-teleskla.ik.local 11/28/2014 17:00 $RII4JBV.com C:\$Recycle.Bin\S-1-5-21-1950629490-3515783127-634922058-2352\ EICAR-ANTIVIRUS-TESTFILE
dew-teleskla.ik.local 11/28/2014 19:07 eicar.com C:\Users\telesklav.m\ EICAR-ANTIVIRUS-TESTFILE
Select All
Purge System
Temporary Unblock
Save & Delete
Pending Tasks
Virus List
Log File
Change Log
Abbildung 6-19: UI – Virenliste

6.2.3.2 *Virusinformation*

Im Fenster **Virusinformationen** (Abbildung 6-20: UI – Virusinformationen
) werden nützliche Informationen zu einer erkannten Infektion angezeigt. Sie können diese Informationen durch Anklicken der Schaltfläche **In die Zwischenablage kopieren** in die Zwischenablage kopieren.

© 2013 IKARUS Security Software GmbH

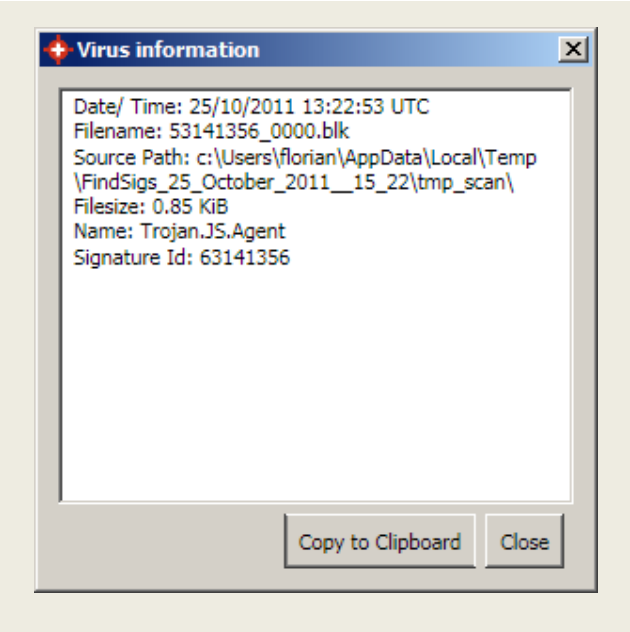


Abbildung 6-20: UI – Virusinformationen

© 2013 IKARUS Security Software GmbH

6.2.4 Logdatei

Im Fenster ***Logdatei*** (Abbildung 5-14) erhalten Sie nützliche Informationen zu den Hintergrundaktivitäten des **IKARUS security.manager-Servers**. Falls Sie Probleme oder ungewöhnliches Verhalten erkennen, stellt das Fenster ***Logdatei*** eine einfache Möglichkeit dar, die Logdatei des **IKARUS security.manager-Servers** von beliebiger Stelle aus mithilfe der **IKARUS security.manager-UI** aufzurufen. Außerdem können Sie festlegen, welche Informationen angezeigt werden sollen: Alarmmeldungen, Warnungen oder lediglich Informationen. Dies kann die Untersuchung von Problemursachen erheblich vereinfachen. Alternativ verwenden Sie zum Durchsuchen der Logdatei das Suchfeld.

6.2.4.1 *Fensteraufbau*

Im oberen Bereich des Logdatei-Fensters können Sie entscheiden, welche Informationen angezeigt und wie oft die Informationen vom Server aktualisiert werden sollen.

Die Schaltflächen besitzen von links nach rechts folgende Funktionen:

- **Alarm**: Blendet Alarme ein/aus.
- **Warnung**: Blendet Warnungen ein/aus.
- **Info**: Blendet Informationen ein/aus.
- **Aktualisieren**: Ruft eine aktualisierte Logdatei vom ISM-Server ab.
- **Automatisch Aktualisieren:** Ruft in vom Benutzer festgelegten Abständen eine aktualisierte Logdatei vom ISM-Server ab.
- **Automatisches Scrollen:** Führt bei automatischer Aktualisierung automatisch einen Bildlauf bis zum Ende der Logdatei aus.
- **Update-Intervall:** Bestimmt den zeitlichen Abstand, in welchem die Logdatei aktualisiert werden soll.

Unter diesem Bereich wird die Logdatei angezeigt. Durch Rechtsklick können Sie innerhalb der Logdatei das Kontextmenü öffnen. Im Kontextmenü können Sie entweder auf "Alle Auswählen" (Auswahl des gesamten Logdateitextes) oder auf "In die Zwischenablage kopieren" drücken.

Im unteren Bereich können Sie in der Logdatei nach einem bestimmten Text suchen. Geben Sie einfach den Text ein, nach dem Sie suchen wollen, in das Textfeld ein und drücken Sie zum Auffinden der Logdatei auf die Loop-Schaltfläche. Die Suche in der Logdatei beginnt nun ab der Position des Textcursors.

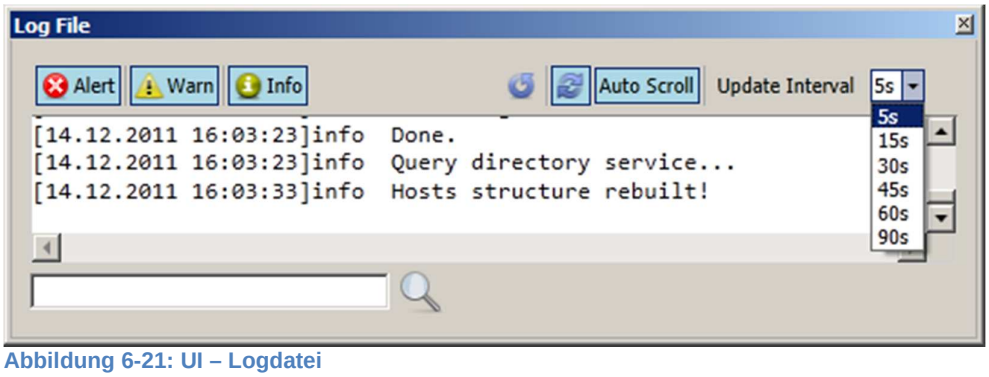


Abbildung 6-21: UI – Logdatei

© 2013 IKARUS Security Software GmbH

6.2.5 Change Log

Im Fenster ***Change Log*** (Abbildung 5-15) erhalten Sie einen Überblick zu den Änderungen, die von einem Benutzer an den Einstellungen vorgenommen wurden, sowie zum Zeitpunkt der jeweiligen Änderung.

6.2.5.1 *Fensteraufbau*

Das **Change Log** (Änderungsprotokoll) lässt sich mithilfe der Aktualisierungsschaltfläche in der rechten oberen Ecke aktualisieren, wodurch sämtliche Änderungen innerhalb des IKARUS security.manager angezeigt werden. Die Liste besitzt folgende Spalten:

- **Id:** Identifizierungsnummer der jeweiligen Änderung.
- **Kategorie:** Zeigt an, wo die Änderung aufgetreten ist.
- **Feld-Id:** Zeigt an, welche Einstellung geändert wurde.
- **Alter Wert:** Zeigt den Wert vor der Änderung an.
- **Neuer Wert:** Zeigt den Wert nach der Änderung an.
- **Zeitstempel:** Zeigt den Zeitpunkt der Änderung.
- **Kommentar:** Zeigt den bei der Anmeldung eingegebenen Kommentar an.

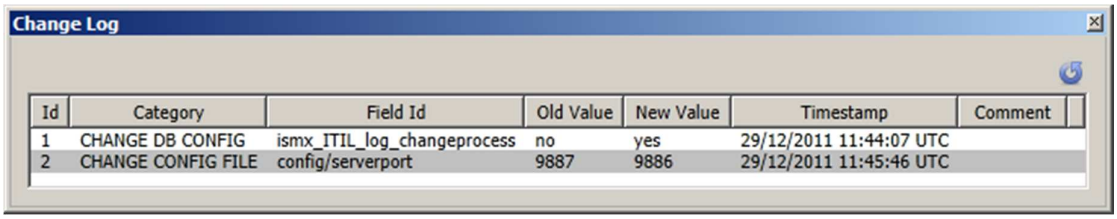


Abbildung 6-22: UI – Change Log

© 2013 IKARUS Security Software GmbH

6.2.6 Die Startseite

Im Fenster ***Startseite*** (Abbildung 5-16) werden allgemeine Informationen zum **IKARUS security.manager-Server**, **statistische Angaben** zu den *Clients* **im** *Verzeichnis* sowie die hinzugefügten *Fileshares* und ihr Online-/Offline-Status gesammelt angezeigt.

6.2.6.1 *Fensteraufbau*

Die Startseite lässt sich mithilfe der Aktualisierungsschaltfläche in der rechten oberen Ecke aktualisieren und besteht aus den folgenden Spalten:

- **Serverinformationen:** Zeigt Informationen zur ISM-Serverversions sowie zum Host an, auf dem der Server läuft.
- **Client-Kurzübersicht:** Bietet einen schnellen Überblick über alle Clients im Verzeichnis
- **Lizenzinformationen:** Zeigt an, wann die Lizenz abläuft und wie viel von Ihrer Lizenzkapazität genutzt wird bzw. noch verfügbar ist.
- **Fileshare-Informationen:** Zeigt Informationen zu Online-/Offline-Fileshares an.
- **Updateübersicht:** Bietet einen schnellen Überblick über jene Versionsnummern, welche der ISM-Server seinen Clients zuweisen kann.

© 2013 IKARUS Security Software GmbH

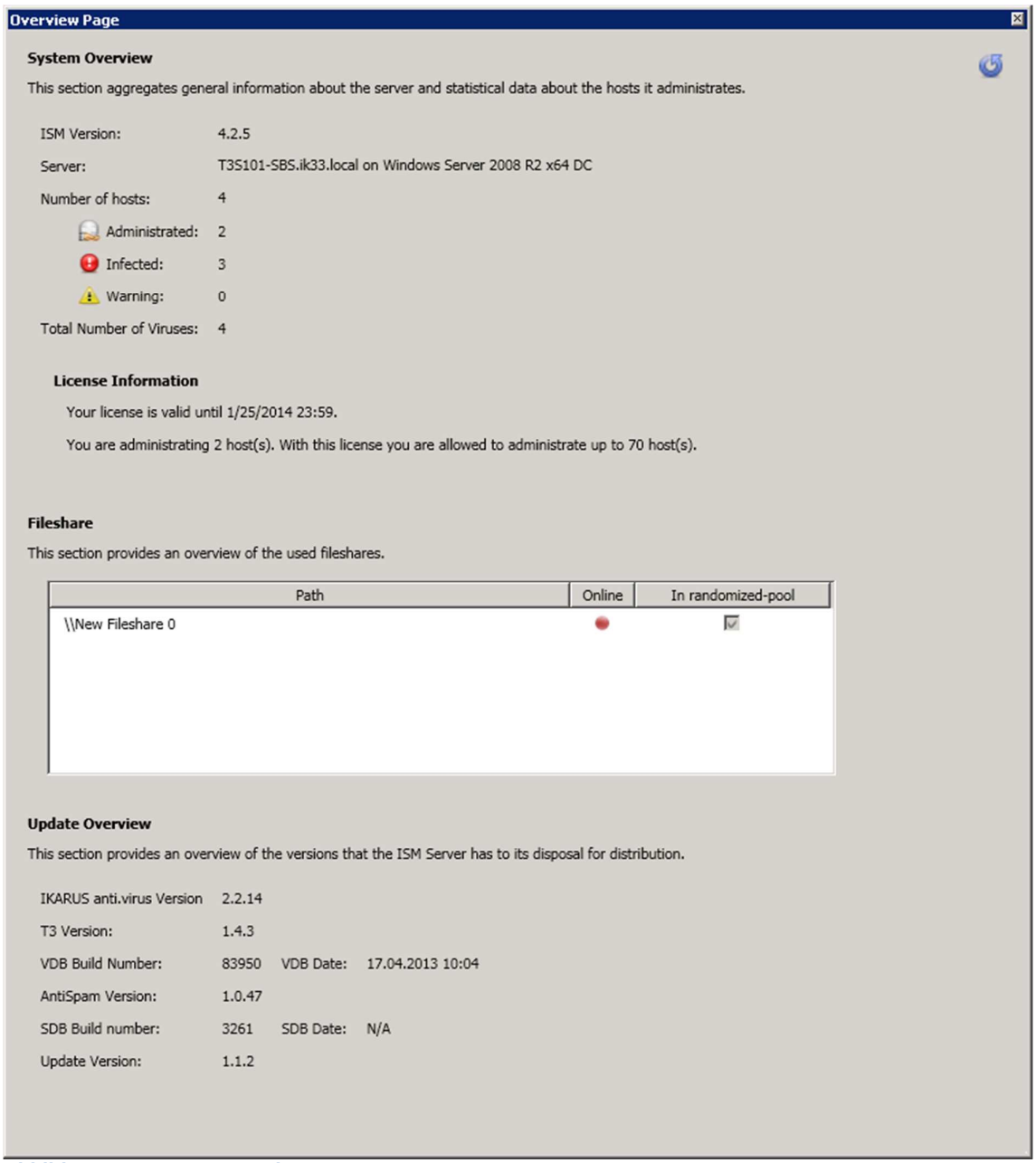

Overview Page
System Overview
This section aggregates general information about the server and statistical data about the hosts it administrates.
ISM Version: 4.2.5
Server: T3S101-SBS.ik33.local on Windows Server 2008 R2 x64 DC
Number of hosts: 4
Administrated: 2
Infected: 3
Warning: 0
Total Number of Viruses: 4
License Information
Your license is valid until 1/25/2014 23:59.
You are administrating 2 host(s). With this license you are allowed to administrate up to 70 host(s).
Fileshare
This section provides an overview of the used fileshares.
Path
Online
In randomized-pool
\\New Fileshare 0
Update Overview
This section provides an overview of the versions that the ISM Server has to its disposal for distribution.
IKARUS anti.virus Version 2.2.14
T3 Version: 1.4.3
VDB Build Number: 83950 VDB Date: 17.04.2013 10:04
AntiSpam Version: 1.0.47
SDB Build number: 3261 SDB Date: N/A
Update Version: 1.1.2

Abbildung 6-23: UI – Startseite

© 2013 IKARUS Security Software GmbH

6.2.7 Eigenschaftsseite

Im Fenster ***Eigenschaftsseite*** (siehe Abbildung 6-24) erhalten Sie einen schnellen Überblick zur **IKARUS anti.virus**-Konfiguration eines *Clients* oder einer Gruppe und zum Zeitpunkt und zur Art und Weise der Aufspielung von Updates auf dem Client bzw. der Gruppe. Sie können diese Einstellungen *client*- oder gruppenweit festlegen und bestimmen, dass alle *Clients* einer Gruppe die Einstellungen vom übergeordneten Element erben. Falls Sie festlegen, dass Einstellungen für eine Gruppe vererbt werden sollen, werden Sie aufgefordert, anzugeben, ob auch die *Clients* in dieser Gruppe die Einstellungen erben sollen; legen Sie hingegen fest, dass Einstellungen für eine Gruppe nicht vererbt werden sollen, dann müssen Sie angeben, ob die *Clients* in dieser Gruppe die Einstellungen ebenfalls nicht erben sollen.

6.2.7.1 *Der Bereich „Update“*

Im **Bereich Update** können Sie angeben, **wann und wie Updates ausgeführt werden** sollen. Sie können pro Gruppe bzw. Host einen spezifischen *Fileshare* festlegen, der jedes Mal um ein Update ersucht wird. Als Voreinstellung für das Beziehen von Updates wird ein *Fileshare* **stichprobenartig aus einer randomisierten Datenbasis ausgewählt**. **Kursiv** dargestellte *Fileshare* sind **zurzeit offline**. Weitere Informationen zu diesem Thema finden Sie in Abschnitt 6.2.14.5.

Wenn Sie **binäre Updates nicht zulassen, werden nur die Virus- und die Spamdatenbank aktualisiert**, **nicht aber IKARUS anti.virus**. Möchten Sie die Statusmeldungen von **IKARUS anti.virus** im Infobereich **ausblenden** (was z. B. auf einem für **Präsentationen** verwendeten Computer erforderlich sein kann, damit das angezeigte Popupfenster das Publikum nicht ablenkt), können Sie erforderlichenfalls das Kontrollkästchen **Statusmeldungen deaktivieren** einschalten.

6.2.7.2 *Sprache*

Im Bereich Sprache können Sie auswählen, in welcher Sprache **IKARUS anti.virus auf dem** ausgewählten Host laufen soll. Wenn sie „**IKARUS anti.virus Spracheinstellungen überschreiben**“ aktivieren, wird auf jeden Fall die von Ihnen gesetzte Sprache gewählt, andernfalls kann die Sprache am Host selbst noch anders gesetzt werden.

6.2.7.3 *Rechteverwaltung*

Der Bereich ***Rechteverwaltung*** ist für *Clients* vorgesehen, die sich außerhalb der *Domäne* befinden, zu der der **IKARUS security.manager-Server** gehört. Da der **IKARUS security.manager-Server** zur Herstellung einer Verbindung und zur Remoteausführung von Binärdateien die erforderlichen Rechte benötigt, können Sie hier Anmeldeinformationen angeben, die auf diesem *Client* über die erforderlichen Rechte zur Durchführung dieser Operationen verfügen.

© 2013 IKARUS Security Software GmbH

6.2.7.4 *Fensteraufbau*

Oben auf dem Fenster werden der Name und das Statussymbol des aktuell ausgewählten Hosts bzw. der aktuell ausgewählten Gruppe angezeigt. Im Fenster sind noch folgende andere Elemente zu sehen:

- **Einstellungen erben:**. Einstellungsvererbung vom übergeordneten Knoten aktivieren/deaktivieren. Diese Einstellung wird automatisch gespeichert, d.h., die Schaltfläche "Speichern" ("Save") muss nicht extra angeklickt werden.
- **IKARUS anti.virus-Konfiguration:** Bestimmt die vom Client verwendete Konfiguration.
- **Updatezeit:** Hier legen Sie die Zeitspanne für die Durchführung von Updates fest.
- **Fileshare:** Hier legen Sie einen konkreten *Fileshare* fest oder wählen einen aus einer randomisierten Datenbasis aus, falls ein Update erforderlich werden sollte.
- **Binary Updates erlauben:** Gestattet Updates der IKARUS anti.virus-Binärdateien. Datenbanken werden auch dann aktualisiert, wenn Sie binäre Updates als Option abwählen.
- **Statusmeldungen im Infobereich deaktivieren:** Unterbindet die Popup-Anzeige von IKARUS anti.virus-Statusmeldungen im Infobereich.
- **Updates von externen Servern erhalten:** Gestattet IKARUS anti.virus das Herunterladen von Updates aus dem Internet, falls der ISM keine Updates bereitstellen kann.
- **Benutzername/Passwort:** Legt die Anmeldeinformationen für die Interaktion mit diesem Client fest. Falls sich der Client nicht in derselben Domäne wie der ISM-Server befindet, müssen diese Angaben unbedingt korrekt sein, damit die Verwaltung dieses Clients einwandfrei funktioniert.
- **Verzeichnisgruppe durchsuchen:** Legt fest, welche Verzeichnisgruppen Änderungen in IKARUS anti.virus durchführen dürfen.
- **Beschränkungen löschen:** Entfernt zuvor festgelegte Beschränkungen für Verzeichnisgruppen.
- **Schaltfläche Speichern:** Speichert diese Einstellungen.
- **Schaltfläche Abbrechen:** Verwirft alle durchgeführten Änderungen.

© 2013 IKARUS Security Software GmbH

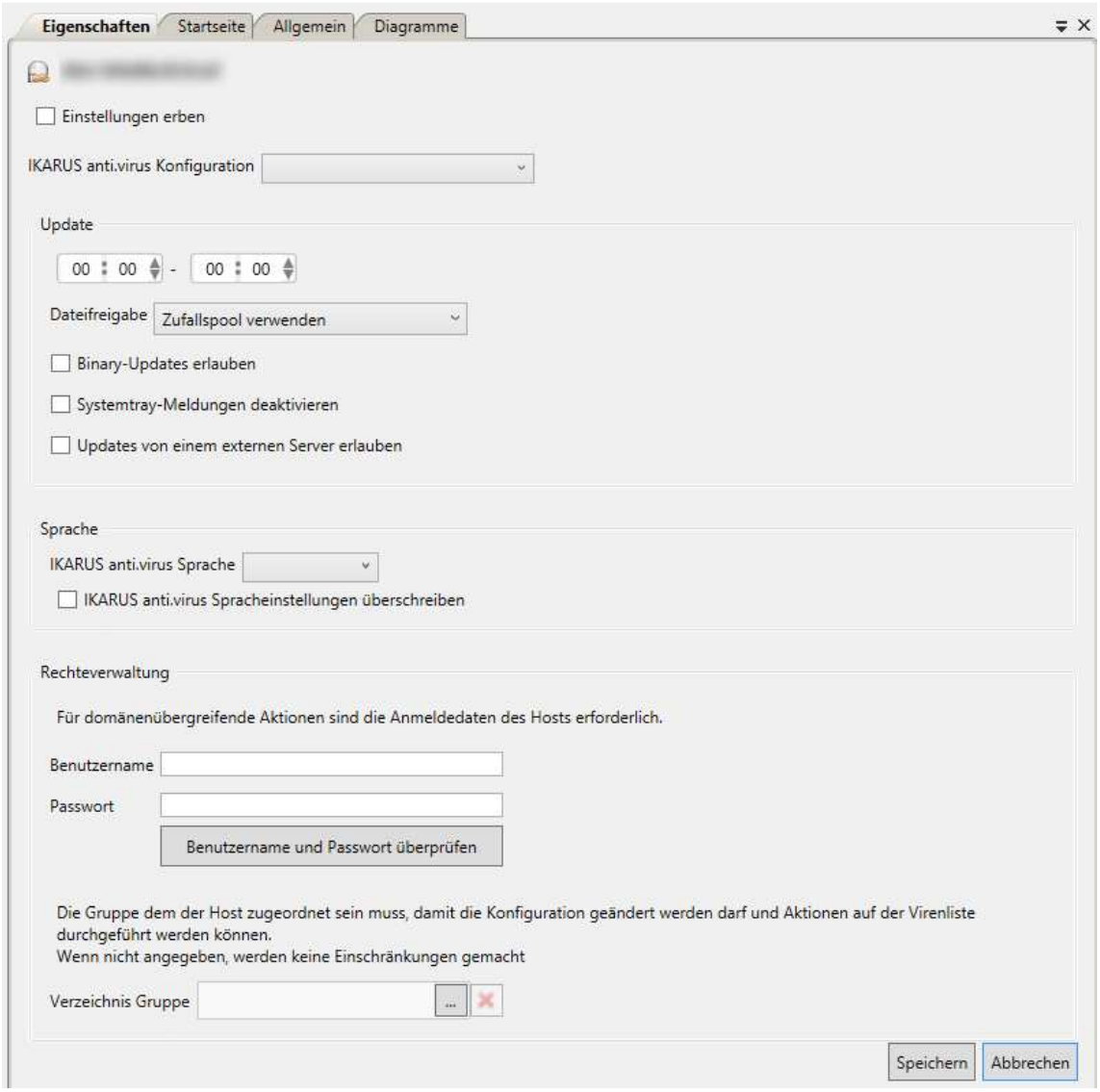


Abbildung 6-24: UI – Eigenschaftsseite

© 2013 IKARUS Security Software GmbH

6.2.8 Seite „Allgemein“ für Gruppen

Auf der Seite ***Allgemein*** (Abbildung 5-18) für Gruppen werden Statistikinformationen zu den *Clients* auf dem gegenwärtig ausgewählten Gruppenknoten angezeigt. Sie erhalten auf diese Weise eine einfache Möglichkeit, den Status vieler *Clients* von zentraler Stelle aus zu untersuchen. Möchten Sie den Status vieler *Clients* untersuchen, die sich nicht in derselben Gruppe befinden, dann können Sie die Funktion *Mehrfachauswahl* des *Verzeichnisses* verwenden.

6.2.8.1 *Fensteraufbau*

Auf der Seite **Allgemein** für Gruppen werden Informationen über alle zu dieser Gruppe gehörenden Hosts zusammengefasst. Oben auf der Seite werden z.B. folgende Informationen angezeigt:

- **Gruppenname:** Zeigt den Namen und die Statussymbole des aktuellen Knotens.
- **Gesamtanzahl der Viren:** Zeigt die Gesamtanzahl der Infektionen auf dem aktuellen Knoten.
- **Anzahl der Clients online:** Zeigt die Gesamtanzahl jener Clients, die auf dem aktuellen Knoten online sind.
- **Anzahl der geschützten Clients:** Zeigt die Gesamtanzahl der überwachten Clients auf dem aktuellen Knoten.
- **Verwaltet:** Zeigt die Gesamtanzahl der verwalteten Clients auf dem aktuellen Knoten.

In der Clientliste unter den allgemeinen Informationen werden sämtliche Hosts der Gruppe detaillierter und mit den folgenden Informationen dargestellt:

- **Statussymbol:** Zeigt das Statussymbol des aktuellen Clients.
- **Name:** Zeigt den Namen des aktuellen Clients.
- **Infektionen:** Zeigt die Anzahl der Infektionen auf dem aktuellen Client.
- **Online:** Zeigt den Onlinestatus dieses Clients.
- **Installierte Dienste:** Zeigt den Installationsstatus jener Dienste, die sich auf diesem Client befinden.
- **Verwaltet:** Zeigt den Verwaltungsstatus dieses Clients an.
- **Letztes Update:** Zeigt das UTC-Datum des letzten Update auf dem aktuellen Client an.
- **Letztes Mal online:** Zeigt das UTC-Datum an, zu welchem dieser Client letztmalig online war.

Zusätzlich ist es möglich die aktuellen Daten der ausgewählten Rechner bzw. Gruppen mit abzurufen. Zu beachten gilt jedoch, dass dieser Prozess **eine längere Zeitspanne beanspruchen kann,** wenn dieser viele Rechner beinhaltet bzw. einige Rechner nicht aktiv sind.

© 2013 IKARUS Security Software GmbH

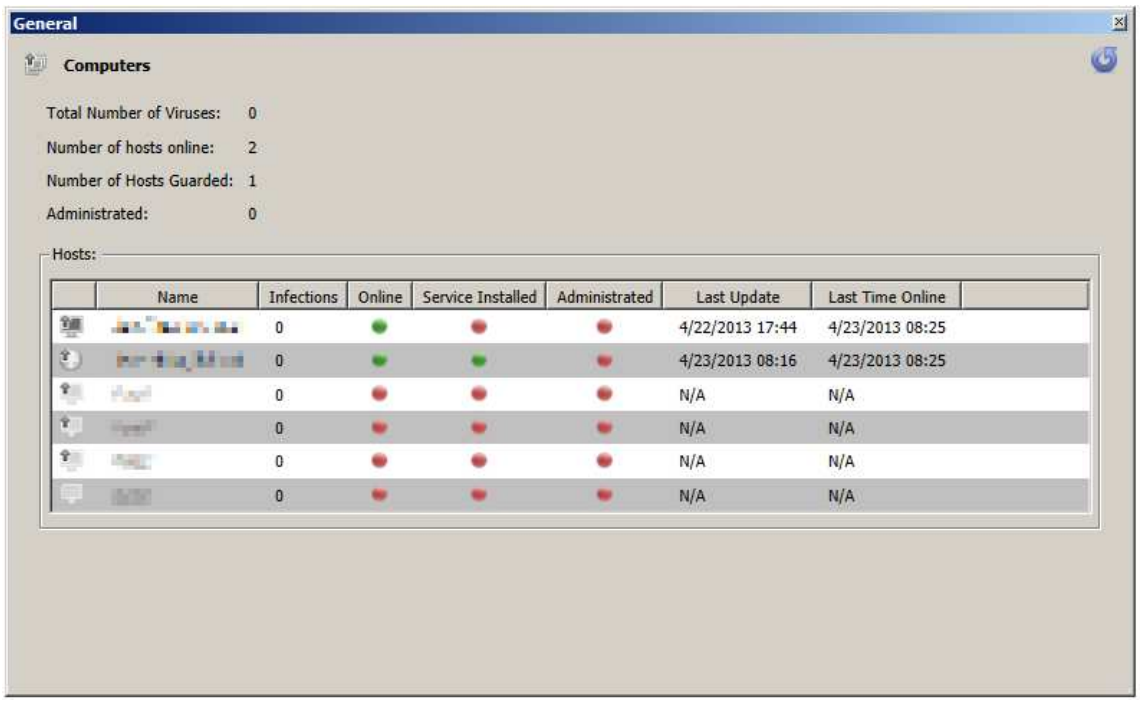


Abbildung 6-25: UI – Seite „Allgemein“ für Gruppen

6.2.8.2 *Symbole*

- Rotes Symbol: „Nein“
- Grünes Symbol: „Ja“

© 2013 IKARUS Security Software GmbH

6.2.9 Seite „Allgemein“ für Clients

Auf der Seite ***Allgemein*** (Abbildung 5-19) für einen *Client* werden ausführliche Informationen zum gegenwärtig ausgewählten *Client* angezeigt.

6.2.9.1 *Fensteraufbau*

Die Allgemeine Seite für Clients ist in folgende Informationsbereiche gegliedert:

- **Allgemein:** Zeigt den Online-, Dienstinstallations- und Verwaltungsstatus des aktuellen Clients an.
- **Update:** Zeigt den Zeitpunkt der letzten Aktualisierung dieses Clients sowie das Datum des nächsten Updatevorgangs an.
- **Versionen:** Zeigt die Versionen von IKARUS anti.virus, der Datenbank, der Scan Engine und des Updates dieses Clients an.
- **Schutz:** Zeigt die Seriennummer, den Scanstatus, die Anzahl der Infektionen sowie die aktivierten bzw. deaktivierten Schutzmechanismen an.

Zusätzlich ist es möglich die aktuellen Daten den ausgewählten Rechner mit ab-zurufen.

Abbildung 6-26: UI – Seite „Allgemein“ für Clients

© 2013 IKARUS Security Software GmbH

6.2.10 Benachrichtigungsleiste

Die Benachrichtigungsleiste (Abbildung 5-20) ist standardmäßig ausgeblendet. Sie wird nur angezeigt, wenn sich Änderungen auf der Virusliste eines Clients ergeben haben. Wenn die **IKARUS security.manager-UI** nicht die aktive Anwendung (d.h. die Anwendung im Vordergrund) ist, blinkt der Eintrag **IKARUS security.manager-UI** in der Windows-Taskleiste, um anzuzeigen, dass Änderungen in der Virusliste aufgetreten sind.

6.2.10.1 *Fensteraufbau*

Abbildung 6-27: UI – Benachrichtigungsleiste

© 2013 IKARUS Security Software GmbH

6.2.11 Diagrammseite

Auf der **Diagrammseite** werden jene 5 Standarddiagramme angezeigt, die zurzeit im **IKARUS security.manager** zur Verfügung stehen. Diese 5 Diagramme lassen sich im **IKARUS security.manager** unter **Optionen** bearbeiten (siehe Abschnitt 6.2.14.7).

Es handelt sich dabei um die folgenden 5 Standarddiagramme:

- Hostverwaltung
- Host-Verfügbarkeit
- Host-Infektionen
- Top-5-Viren sowie
- Virus nach Betriebssystem

Auf dieser Seite werden nicht nur die Diagramme angezeigt, sondern auch der Zeitpunkt ihrer Erstellung. Die Diagramme lassen sich durch Anklicken der Schaltfläche **Aktualisieren** rechts oben leicht aktualisieren.

Die Schaltfläche links neben der Aktualisierungsschaltfläche dient zur Erstellung eines PDF-Berichts für die Diagramme. Dieser Bericht enthält ausschließlich jene Diagramme, welche gegenwärtig auf der **Diagrammseite** dargestellt werden. Auch der PDF-Bericht lässt sich im **IKARUS security.manager** unter **Optionen** nach Wunsch anpassen.

Anmerkung: Zum Betrachten des PDF-Reports muss ein PDF-Viewer installiert sein.
Anmerkung: Weitere Informationen zum Bearbeiten und Anpassen der Diagramme finden Sie im **IKARUS security.manager** unter **Optionen** (siehe 6.2.14).
Anmerkung: Als Mindestvoraussetzung für die Anzeige der Diagramme muss **mindestens Version 7 des Internet Explorer** installiert sein. Zur Gewährleistung des vollen Funktionsumfangs empfehlen wir den **Internet Explorer Version 9**. Bitte beachten Sie, dass zur Berechnung der Diagramme JavaScript aktiviert sein muss.

© 2013 IKARUS Security Software GmbH

6.2.11.1 *Fensteraufbau*

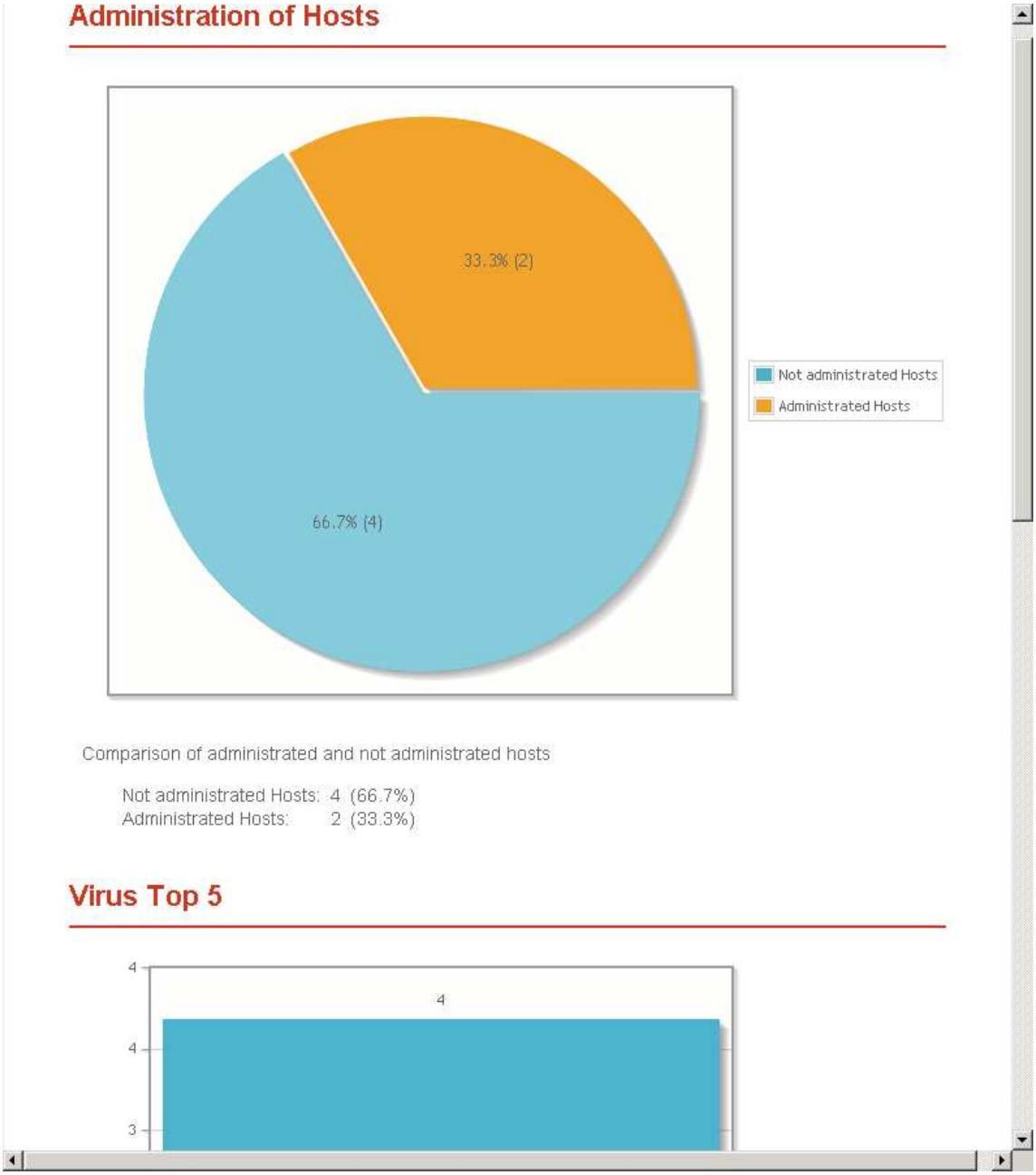


Abbildung 6-28 UI –Diagrammseite

© 2013 IKARUS Security Software GmbH

6.2.12 Globale Startseite

Diese Seite dient zur Übersicht aller eingetragenen **IKARUS security.manager-Server** (siehe Abbildung 6-29), welche nur im Management-Modus verfügbar ist. Es werden die wichtigsten Informationen angezeigt wie die Anzahl der Computer, wieviele Rechner administriert werden bzw. infiziert oder nicht aktuell sind. Des Weiteren ist die aktuelle Lizenz, die Version und ein Zeitstempel bezüglich der letzten Aktualisierung dargestellt.

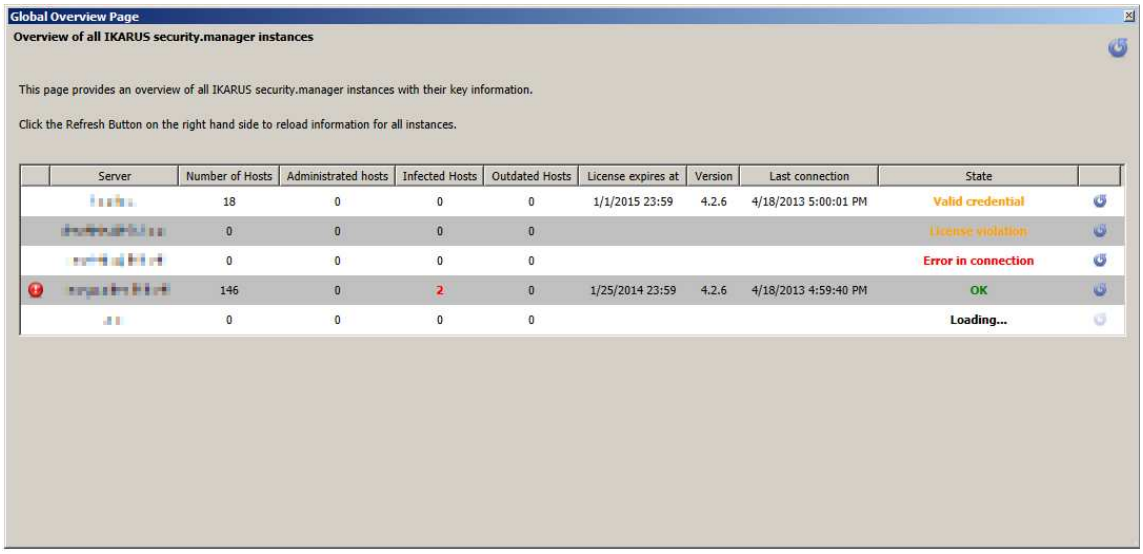

Global Overview Page
Overview of all IKARUS security.manager instances
This page provides an overview of all IKARUS security.manager instances with their key information.
Click the Refresh Button on the right hand side to reload information for all instances.
Server
Number of Hosts
Administrated hosts
Infected Hosts
Outdated Hosts
License expires at
Version
Last connection
State
18 0 0 0 1/1/2015 23:59 4.2.6 4/18/2013 5:00:01 PM Valid credential
0 0 0 0 License violation
0 0 0 0 Error in connection
146 0 2 0 1/25/2014 23:59 4.2.6 4/18/2013 4:59:40 PM OK
0 0 0 0 Loading...

Abbildung 6-29 UI – Globale Startseite

Die Daten der **IKARUS security.manager-Server** werden **nicht** automatisch aktualisiert. Die zuletzt abgerufenen Verbindungsdaten werden gespeichert und stehen nach der nächsten Anmeldung zur Verfügung. Jeder **IKARUS security.manager-Server** kann individuell aktualisiert werden, indem auf in der dementsprechenden Zeile gedrückt wird. Für die Aktualisierung aller Einträge in der Globalen Startseite kann rechts oben genutzt werden.

Nach jeder Aktualisierung wird ein aktueller Status bereitgestellt, der Auskunft über mögliche Probleme gibt:

- **Lade...**
  Die Daten werden abgerufen.
- **OK**
  Informationen wurden erfolgreich geladen.
- **Verbindungsfehler**
  Die Verbindung konnte nicht aufgebaut werden.
- **Zugangsdaten gültig**
  Die Zugangsdaten sind gültig
- **Lizenzverletzung**
  Ein Problem mit der Lizenz ist aufgetreten und sollte geklärt werden.
- **Verbindung zum letzten Mal vor über 2 Tagen aufgebaut**
- **Verbindung noch nie aufgebaut**

© 2013 IKARUS Security Software GmbH

Wird eine ältere Version als 4.2.x verwendet, so können diese **IKARUS security.manager-Server nicht mit dem Management-Modus verwaltet werden**. Dennoch werden diese in der globalen Übersichtsseite angezeigt.

Weiters ist es möglich mit Hilfe der rechten Maustaste das Kontextmenü mit den folgenden Einträgen aufzurufen (siehe Abbildung 6-30).

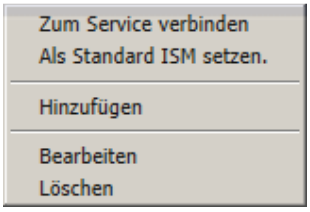


Abbildung 6-30 UI – Globale Startseite - Kontextmenü

- **Zum Service verbinden**
  Wechselt zu dem aktuell selektierten **IKARUS security.manager-Server** und beendet die Verbindung zu dem zuvor ausgewählten **IKARUS security.manager-Server**.
- **Als Standard ISM setzen**
  Der aktuell selektierte **IKARUS security.manager-Server** wird als Standard-Server beim Neustart gesetzt.
- **Hinzufügen**
  Fügt einen neuen **IKARUS security.manager-Server** zu der Liste. Weitere Informationen entehmen Sie aus dem Kapitel 6.2.16.1.2.
- **Bearbeiten**
  Die Anmeldeeigenschaften des aktuell selektierten **IKARUS security.manager-Server** werden editiert. Der Bearbeitungsdialog ist nicht verfügbar, wenn der selektierte **IKARUS security.manager** bereits eine Verbindung aufgebaut hat oder sich im Verbindungsaufbau befindet. Weitere Informationen entehmen Sie aus dem Kapitel 6.2.16.1.1.
- **Löschen**
  Der aktuell selektierte **IKARUS security.manager-Server** wird dauerhaft aus der Verwaltungsliste gelöscht. Ein Verbindungsaufbau ist daher nicht mehr möglich. Der aktuell verbundene bzw. der Standard **IKARUS security.manager-Server** kann nicht aus der Liste entfernt werden.

© 2013 IKARUS Security Software GmbH

6.2.13 IKARUS anti.virus -Konfigurationen

Im Fenster ***IKARUS anti.virus -Konfigurationen*** (Abbildung 5-21) sind alle vorhandenen **IKARUS anti-virus**-Konfigurationen sowie die Clients aufgelistet, die diese Konfigurationen verwenden. Sie können eine Konfiguration bearbeiten, indem Sie auf die Schaltfläche ***Ausgewählte Konfiguration bearbeiten*** klicken oder auf die gewünschte Konfiguration doppelklicken. Weitere Informationen zur Konfiguration der **IKARUS anti.virus** und zu den verschiedenen Einstellmöglichkeiten finden Sie im **IKARUS anti.virus**-Handbuch.

6.2.13.1 *Fensteraufbau*

Auf der Symbolleiste des Konfigurationsdialogs können die folgenden Aktionen ausgeführt werden:

- Konfiguration hinzufügen
- Ausgewählte Konfiguration bearbeiten
- Ausgewählte Konfiguration löschen
- Konfiguration importieren
- Ausgewählte Konfiguration exportieren

In der ersten Liste des Dialogfelds (siehe Abbildung 5-26) werden sämtliche verfügbaren Konfigurationen des IKARUS security.manager angezeigt. Durch Öffnen der zweiten Liste lassen sich außerdem sämtliche Hosts betrachten, welche die ausgewählte Konfiguration verwenden.

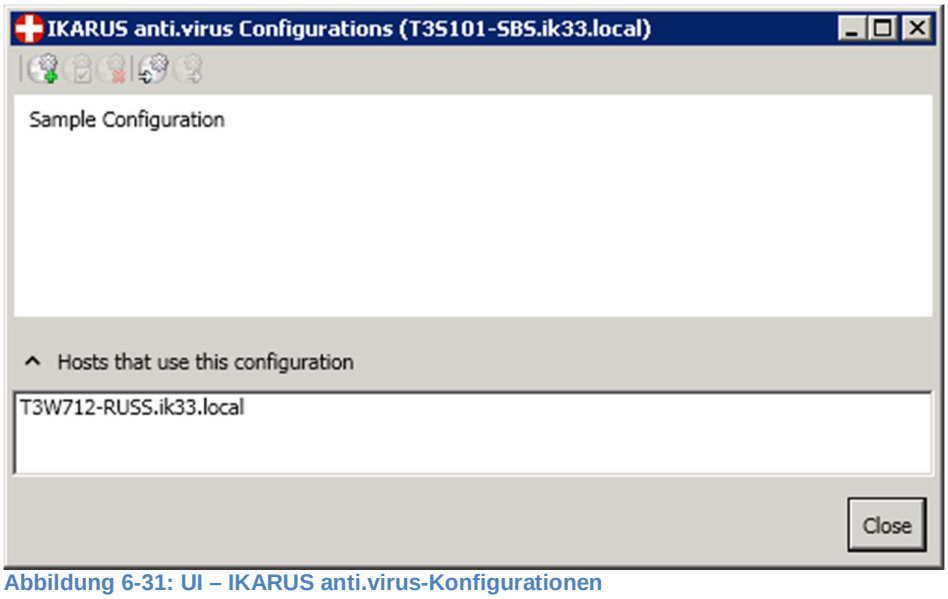


Abbildung 6-31: UI – IKARUS anti.virus-Konfigurationen

6.2.13.2 *Allgemein*

Auf der Registerkarte **Allgemein** des Dialogfeldes **IKARUS anti.virus-Konfiguration** können alle erforderlichen Schutzeinstellungen aktiviert oder deaktiviert werden. Die Konfiguration kann durch Anklicken der Schaltflächen OK oder

© 2013 IKARUS Security Software GmbH

Speichern gespeichert werden. Bei Anklicken der Schaltfläche Abbrechen werden die vorgenommenen Änderungen verworfen. Außerdem wird bei Anklicken der Schaltflächen **OK** bzw. Abbrechen das Dialogfeld **IKARUS anti.virus-Konfiguration** geschlossen.
Auf der Registerkarte **Allgemein** können folgende Einstellungen vorgenommen werden:

- **Systemschutz aktivieren:** Aktiviert bzw. deaktiviert den Systemschutz (bei Deaktivierung werden auch alle anderen Optionen deaktiviert)
- **Schutz von Internet-Downloads aktivieren:** Aktiviert bzw. deaktiviert den Schutz für aus dem Internet heruntergeladene Inhalte
- **Schutz vor Spyware aktivieren:** Aktiviert bzw. deaktiviert den Spyware-Schutz
- **Schutz vor Dialern aktivieren:** Aktiviert bzw. deaktiviert den Schutz vor Dialern

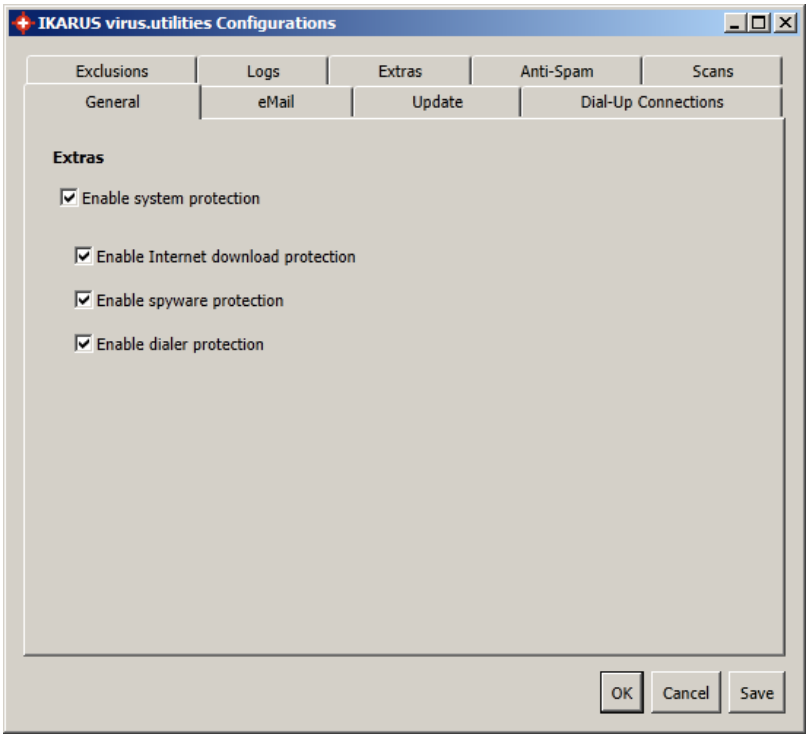


Abbildung 6-32: „IKARUS anti.virus-Konfiguration“, Registerkarte „Allgemein“

6.2.13.3 *E-Mail*

Auf der Registerkarte **E-Mail** des Dialogfeldes **IKARUS anti.virus-Konfiguration** kann der E-Mail-Schutz für den Client aktiviert oder deaktiviert werden. Außerdem kann der Administrator verschiedene Einstellungen dazu vornehmen, z.B. wo in der E-Mail der Scanbericht eingefügt werden soll. Bei ein- und ausgehenden E-Mails kann der Scanbericht wahlweise am Anfang oder am Ende einer Mail eingefügt oder ganz weggelassen werden.

Im Bereich **E-Mail** können folgende Einstellungen konfiguriert werden:

© 2013 IKARUS Security Software GmbH

- **E-Mail-Schutz aktivieren:** Aktiviert bzw. deaktiviert den Schutz von E-Mails
- **Infizierte Anhänge speichern?:** Legt fest, ob clientseitig infizierte Anhänge gespeichert werden sollen
- **Scanstatus:** Zeigt den Scanstatus an
- **Für eingehende E-Mails:** Legt jene Position fest, an welcher der Scanbericht in eingehende E-Mails eingefügt werden soll
- **Für ausgehende E-Mails:** Legt jene Position fest, an welcher der Scanbericht in ausgehende E-Mails eingefügt werden soll

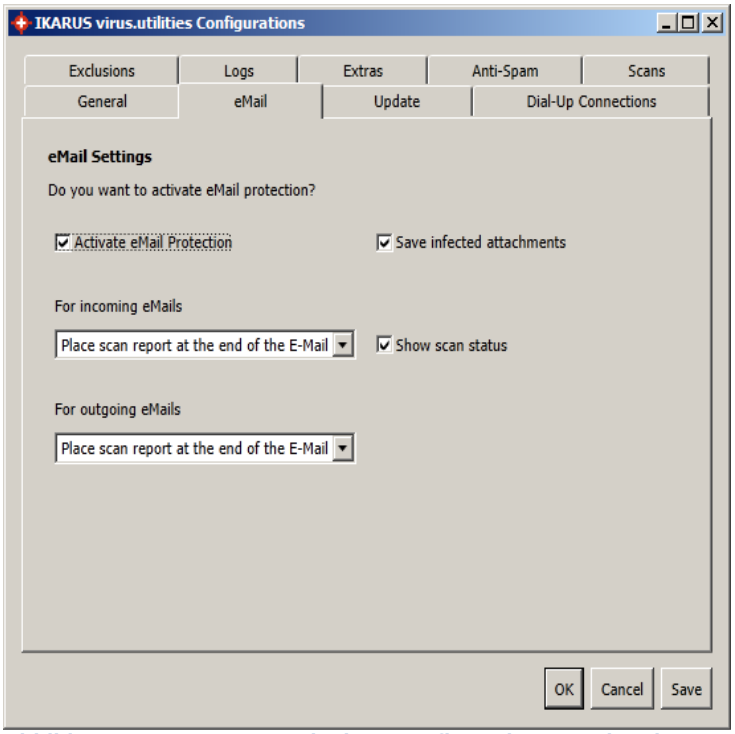


Abbildung 6-33: „IKARUS anit.virus-Konfiguration“, Registerkarte „E-Mail“

© 2013 IKARUS Security Software GmbH

6.2.13.4 *Update*

Alle für die Aktualisierung von **IKARUS anti.virus** erforderlichen Einstellungen können auf der Registerkarte **Update** vorgenommen werden. Die hier angegebenen Informationen sind insbesondere dann von Bedeutung und müssen unbedingt korrekt sein, wenn Sie einen **Proxyserver** verwenden.

Auf der Registerkarte **Update** können folgende Einstellungen vorgenommen werden:

- **Automatisch suchen:** Aktiviert die automatische Suche
- **Produktupdates automatisch installieren:** Produktupdates werden automatisch installiert
- **Proxyserver verwenden:** Aktiviert/deaktiviert die Verwendung eines Proxyservers
- **Server:** Adresse des Proxyservers
- **Port:** Port des Proxyservers
- **Benutzername:** Der Benutzername für den Proxyserver (falls erforderlich)
- **Passwort:** Das Passwort für den Proxyserver (falls erforderlich)

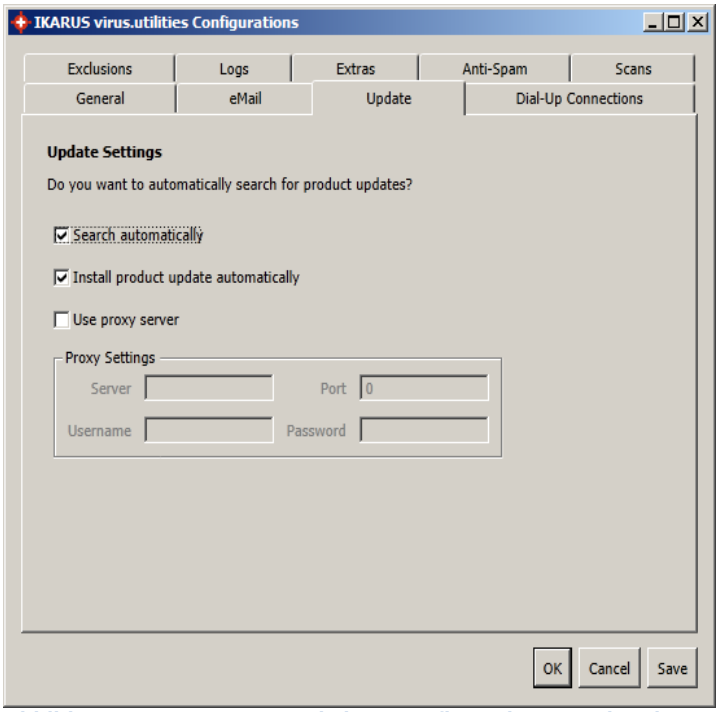


Abbildung 6-34: „IKARUS anti.virus-Konfiguration“, Registerkarte „Update“

6.2.13.5 *Dial-Up-Verbindungen*

Sollten Sie noch eine Modem- oder Einwahlverbindung verwenden, dann können Sie die erforderlichen Verbindungseinstellungen auf der Registerkarte **Dial-Up-Verbindungen** angeben. Mit den hier gemachten Einstellungen konfigurieren Sie die automatische Wählfunktion für die Aktualisierung von **IKARUS anti.virus**. Sie können einen Zeitraum angeben, in dem die automatische Updatefunktion (AutoUpdate) selbsttätig einen Wählvorgang ausführt und eine Verbindung mit dem Internet herstellt (vorausgesetzt, die Dial-Up-Verbindung wurde ausgewählt).

© 2013 IKARUS Security Software GmbH

Auf der Registerkarte **Dial-Up-Verbindungen** können folgende Einstellungen vorgenommen werden:

- **Modem/Dial-Up-Verbindung:** Geben Sie hier die Bezeichnung des Modems- bzw. der Einwahlverbindung ein
- **Automatisches Einwählen aktivieren:** Aktiviert automatisches Einwählen.
- **Zeitrahmen einstellen:** Legt den Zeitrahmen für die automatische Herstellung der Verbindung fest

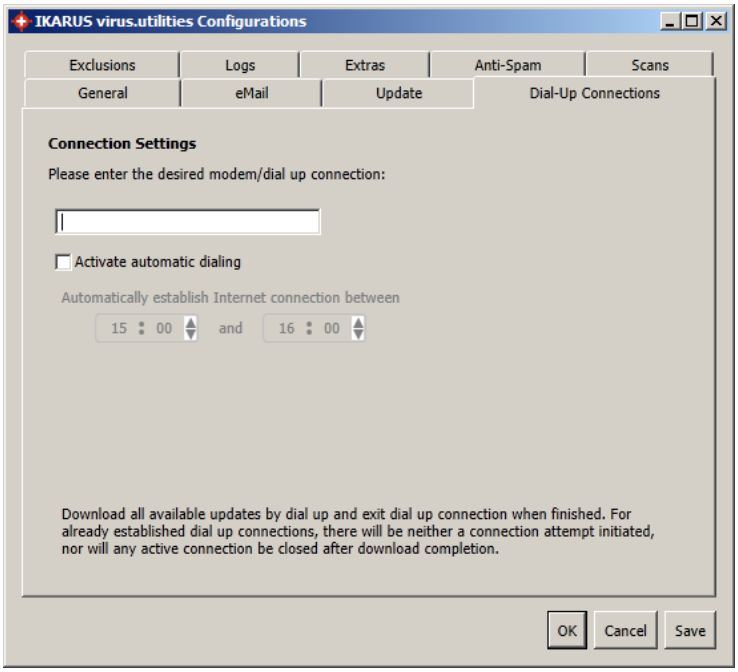


Abbildung 6-35: „IKARUS anti.virus -Konfiguration“, Registerkarte „Dial-Up-Verbindungen“

6.2.13.6 *Ausnahmen*

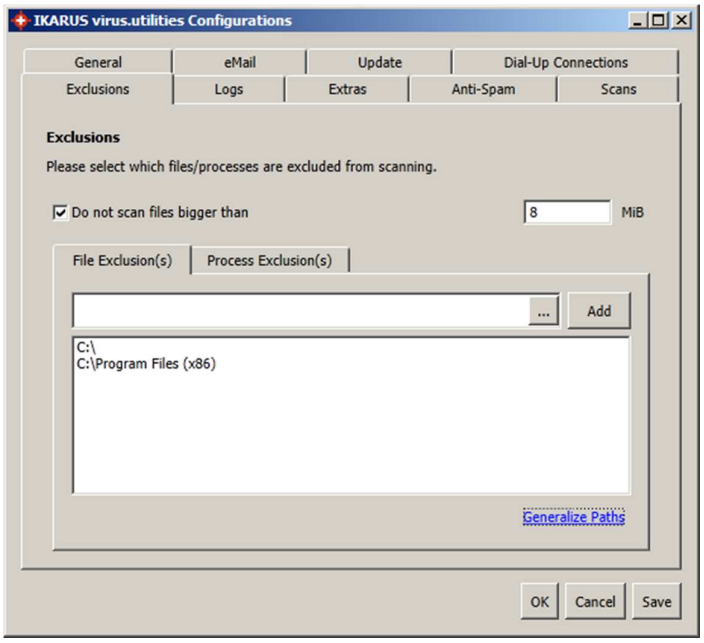
Auf der Registerkarte **Ausnahmen** können Sie festlegen, welche Dateien und Prozesse vom Virenscan ausgenommen werden sollen. Dies kann insbesondere in solchen Fällen recht praktisch sein, in denen Sie einen Dienst, der bereits erhebliche Systemressourcen benötigt (MP3-Dateien, Urlaubsfotos usw.), oder ein bestimmtes Verzeichnis vom Scan ausnehmen möchten.

Wenn Sie Umgebungsvariablen für bestimmte Ordner oder Laufwerke festgelegt haben, für die Sie systemweit eine Ausnahme festlegen möchten, können Sie diese Funktion anstelle des jeweiligen Pfades verwenden. Dabei schließt **IKARUS anti.virus** auch dann den jeweils korrekten Pfad vom Scan aus, wenn dieser auf den verschiedenen Hosts unterschiedlich ist. Im Textfeld können Sie mit **Strg+Leertaste** alle Umgebungsvariablen des aktuellen Systems (d. h. desjenigen Systems, auf dem die Benutzeroberfläche installiert ist) anzeigen.

© 2013 IKARUS Security Software GmbH

Auf der Registerkarte **Ausnahmen** lassen sich die folgenden Einstellungen konfigurieren:

- **Feld für MiB-Anzahl:** Aktiviert bzw. deaktiviert das Scannen von Dateien, welche die hier angegebene Größe übersteigen.
- **Schaltfläche Hinzufügen:** Fügt der Registerkarte **Ausnahmen** Pfade und Umgebungsvariablen hinzu.
- **Ausnahmenliste:** Es handelt sich hier um Variable bereits ausgewählter Pfade bzw. Umgebungen. Nach Auswählen von Prozessausnahmen werden hier die ausgenommenen Prozesse angezeigt.
- **Pfade verallgemeinern:** Falls Sie nicht sicher sind, ob eine Umgebungsvariable für einen bestimmten Pfad besteht, können Sie Pfade generalisieren anklicken. Diese Funktion gilt nicht für Prozessausnahmen.
    - **Alter Pfad:** Der von Ihnen angegebene Pfad.
    - **Neuer Pfad:** Der durch ein Umgebungsvariable ersetzte Pfad.
    - **Änderungen annehmen:** Bitte ankreuzen, falls Sie die Änderungen übernehmen wollen.



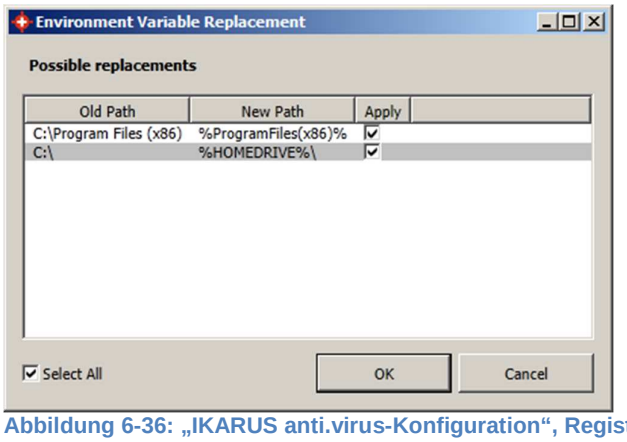


Abbildung 6-36: „IKARUS anti.virus-Konfiguration“, Registerkarte „Ausnahmen“ (Prozessausnahme)

© 2013 IKARUS Security Software GmbH

6.2.13.7 *Logs*

Auf der Registerkarte **Logs** kann der Administrator definieren, welche Aktionen in den
IKARUS anti.virus protokolliert werden sollen.

Auf der Registerkarte **Logs** können die folgenden Einstellungen geändert werden:

- **Systemüberwachung in der Hauptlogdatei protokollieren:** Protokolliert die Systemüberwachung in der Hauptlogdatei von **IKARUS anti.virus**.
- **Protokolle für Scans anlegen:** Aktivieren Sie diese Option, falls Logs für die Scans angelegt werden sollen.
- **Beim Scannen alle Daten aufzeichnen:** Aktivieren Sie diese Option, falls alle Daten aufgezeichnet werden sollen.
- **Überschreiben von Protokolldateien aktivieren:** Beim Starten eines neuen Scans wird das bereits vorhandene Protokoll überschrieben.

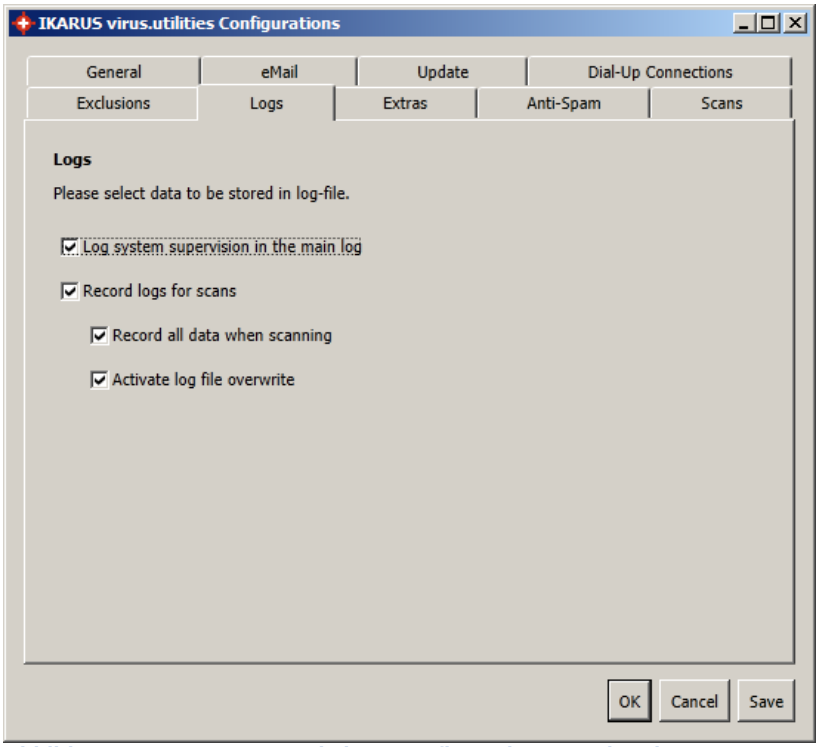


Abbildung 6-37: „IKARUS anti.virus-Konfiguration“, Registerkarte „Logs“

6.2.13.8 *Extras*

Mithilfe der Registerkarte **Extras** können Sie IKARUS anti.virus auf seine Standardwerte zurücksetzen und den Systemschutz für die Startphase Ihres Betriebssystems aktivieren. Auf der Registerkarte **Extras** lässt sich der Systemschutz so einstellen, dass er beim Hochfahren aktiviert wird; eben lassen sich darauf sämtliche Einstellungen auf die Standardwerte zurücksetzen.

© 2013 IKARUS Security Software GmbH

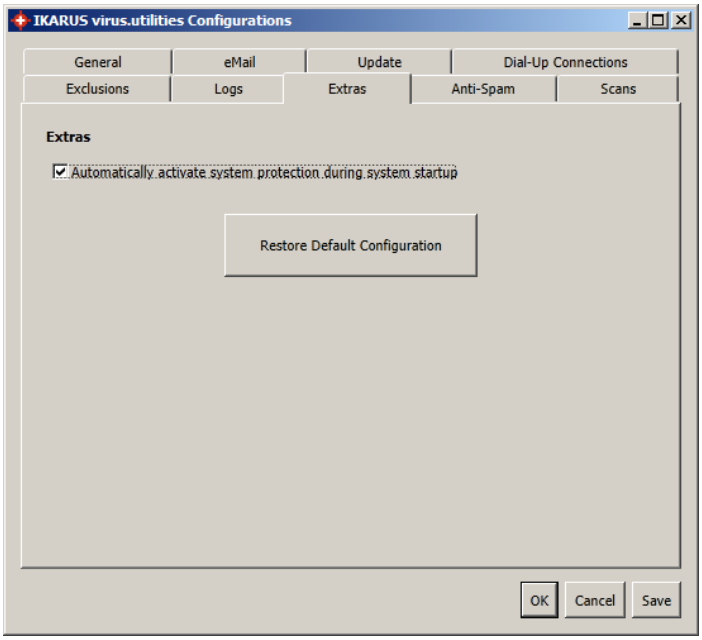


Abbildung 6-38: „IKARUS anti.virus-Konfiguration“, Registerkarte „Extras“

6.2.13.9 *Anti-Spam*

Das **IKARUS-Modul Anti-Spam** gestattet Ihnen das Filtern von E-Mails, die mit Outlook, Outlook Express oder Windows Mail empfangen werden. Zur Aktivierung des Spamschutzes klicken Sie in den Einstellungen von **IKARUS anti.virus** einfach auf die Option **Anti-Spam aktivieren**.

Beim nächsten Programmneustart wird das Anti-Spam-Modul dann aktiviert. Zur Einstellung der Spamauswertung klicken Sie bitte auf die gelben und roten Steuerelemente. Dabei bezeichnet der gelbe Bereich möglichen und der rote tatsächlichen Spam.

Unten auf der Registerkarte können Sie jene Aktion festlegen, die beim Empfang von Spammails ausgeführt werden soll:

- Die Betreffzeile der E-Mail erhält den Zusatz "Möglicher Spam", oder
- Die E-Mail wird in den Ordner Ihres Mailclients für Junk-E-Mail verschoben.

E-Mails, die möglicherweise Spam sind, werden stets in der Betreffzeile entsprechend gekennzeichnet und verbleiben im Posteingang Ihres Mailclients.

© 2013 IKARUS Security Software GmbH

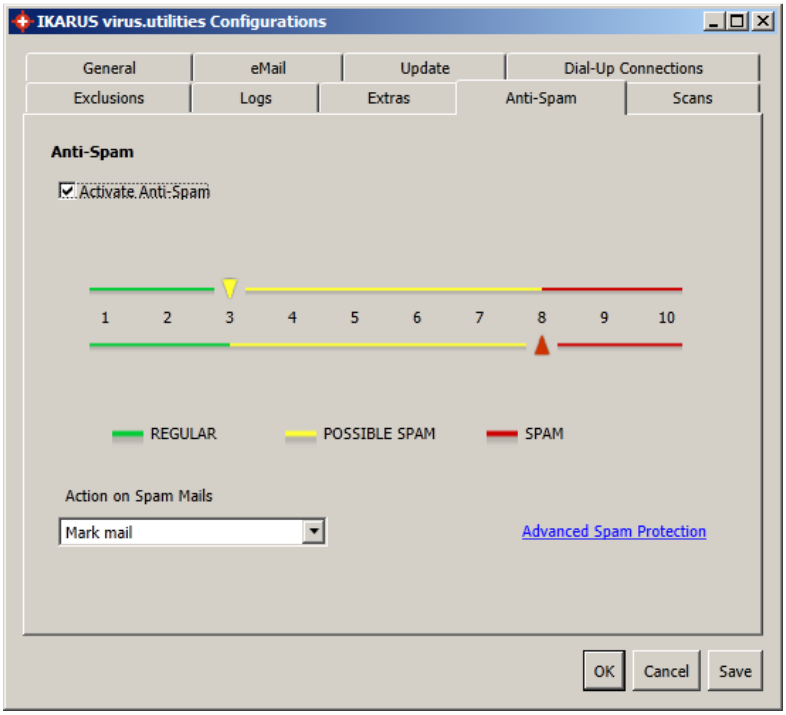


Abbildung 6-39: „IKARUS anti.virus-Konfiguration“, Registerkarte „Anti-Spam“

Erweiterter Spamschutz:
Hier können Sie Ihren eigenen Spamfilter konfigurieren. Dazu können Sie Spamregeln für Absender, Empfänger, Betreffzeile und Inhalte von E-Mails definieren.

Folgende Einstellungen können vorgenommen werden:

- **E-Mail-Bereich:** Hier können Sie festlegen, welcher Bereich (z.B. Absender, Empfang, Betreff oder Inhalt) für die Spamregeln verwendet werden soll
- **Inhalt:** Zu analysierender Inhalt
- **Typ:** E-Mail-Typ, der eine normale E-Mail, möglicher Spam bzw. Spam sein kann
- **Schaltfläche hinzufügen:** Durch Anklicken wird der erweiterte Spamschutz aktiviert
- **Spalte E-Mail-Bereich:** Liste zum Eintragen von E-Mail-Bereichen
- **Spalte Inhalt:** Liste zum Eintragen von Inhalten
- **Spalte Typ:** Liste zum Eintragen von E-Mail-Typen
- **Spalte Rangordnung:** Mit Hilfe dieser Schaltflächen können Regeln gelöscht oder an andere Orte verschoben werden:
    - Erweiterten Spamschutz löschen
    - Zum Anfang verschieben
    - Nach oben verschieben
    - Nach unten verschieben
    - Zum Ende verschieben

© 2013 IKARUS Security Software GmbH

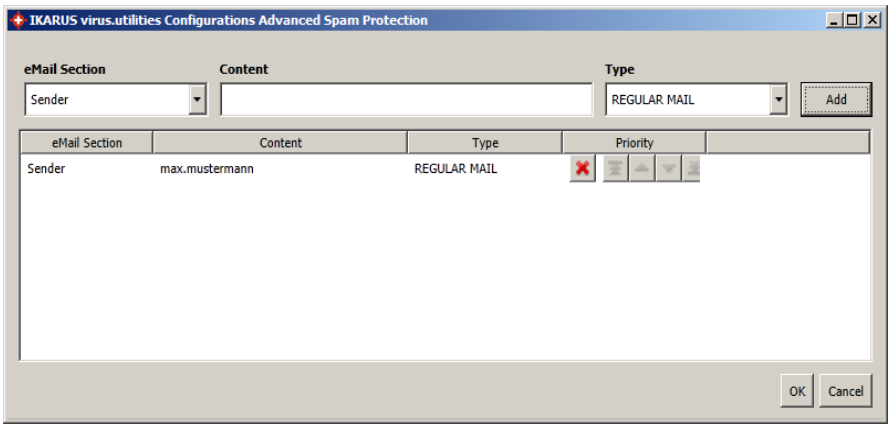


Abbildung 6-40: Dialogfeld „Konfiguration erweiterter Spamschutz“

6.2.13.10 *Scans*

Scans können in IKARUS anti.virus wahlweise automatisch ausgeführt oder manuell gestartet werden. Sie können beliebig viele Scans hinzufügen und verwalten.

Voreingestellte Standardscans (Presets):

- **Schneller Systemscan:** Mithilfe dieses Standardscans scannen Sie das Windows-Installationsverzeichnis. Die meisten Schadprogramme wie Viren und Trojaner sind in diesem Verzeichnis zu finden und können dort schnell und einfach erkannt werden.
- **Systempartition:** Bei Auswahl dieses Standardscans scannt **IKARUS anti.virus** das Laufwerk, auf dem Ihr Betriebssystem installiert ist. Der Scan erstreckt sich auf alle Archive, Verzeichnisse, Ordner und Dateien auf diesem Laufwerk.
- **Gesamter Host:** Mithilfe dieses Standardscans werden alle Laufwerke auf Ihrem Computer von **IKARUS anti.virus** gescannt.
- **Entfernbare Medien:** Mithilfe dieses Standardscans werden alle externen Laufwerke (USB-Sticks, CD-ROM-Laufwerke usw.) gescannt.

© 2013 IKARUS Security Software GmbH

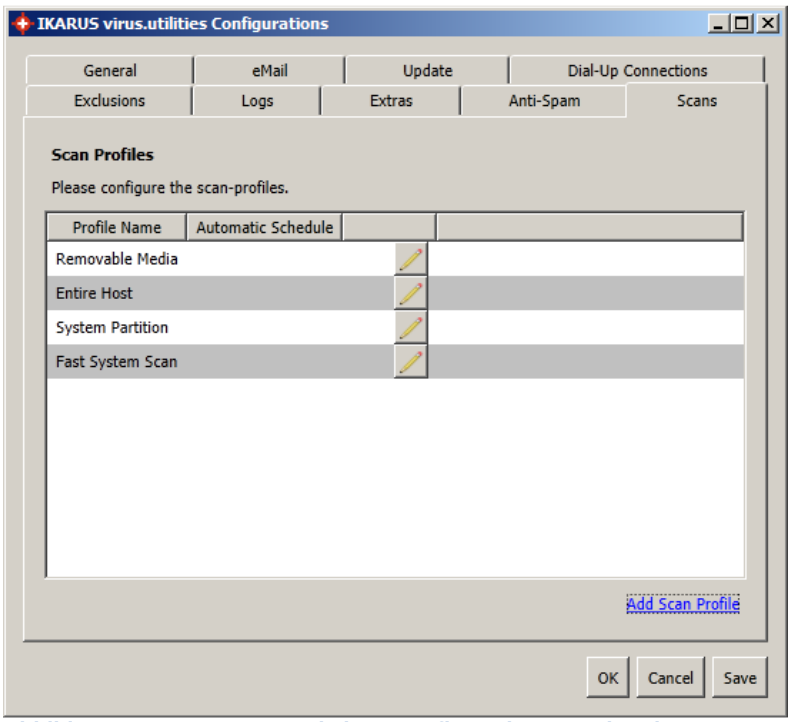


Abbildung 6-41: „IKARUS anti.virus-Konfiguration“, Registerkarte „Scans“

Zur Konfiguration eines neuen Scanprofils klicken Sie auf **Scan-Profil hinzufügen**. Sie können für den Scan nun einen beliebigen Namen eingeben. Klicken Sie auf **Durchsuchen**, um die zu scannenden Ordner, Dateien usw. auszuwählen. Falls erforderlich, können Sie auch die automatische Ausführung von Scans festlegen.

Für den automatischen Scan kann ein beliebiger Zeitpunkt festgelegt werden (z. B. jeden Freitag um 0:00 Uhr). Gescannt werden nur die Bereiche, die vom Benutzer ausgewählt wurden.

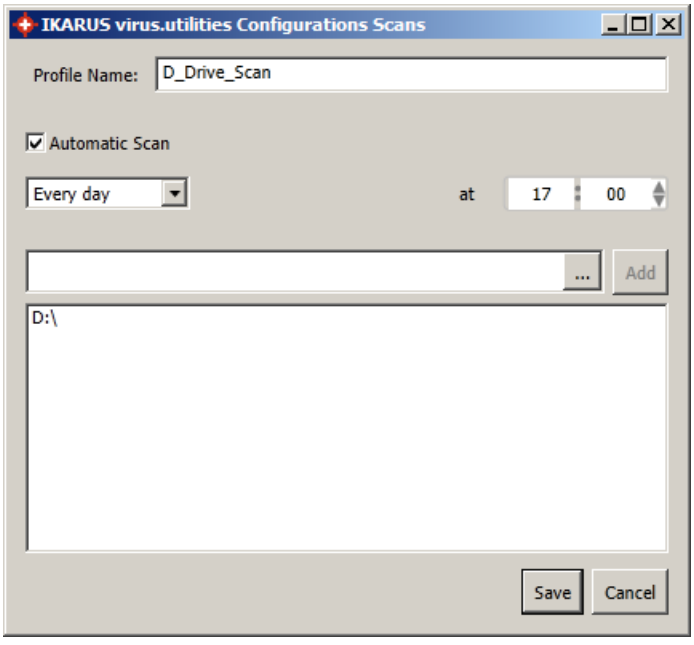


Abbildung 6-42: „IKARUS anti.virus-Konfiguration“, Dialogfeld „Scan-Profil hinzufügen“

© 2013 IKARUS Security Software GmbH

6.2.14 IKARUS security.manager-Einstellungen

Im Fenster ***IKARUS security.manager-Einstellungen*** (Abbildung 5-22) werden Einstellungen für den **IKARUS security.manager-Server** angezeigt. Es umfasst fünf Registerkarten: ***Allgemein***, ***E-Mail Benachrichtigungen, Update, Fileshare, LDAP und Diagramme***. Änderungen an diesen Einstellungen werden übernommen, wenn die Schaltflächen ***OK*** oder ***Anwenden*** unten im Fenster angeklickt werden. Fehlen Informationen oder wurden ungültige Angaben gemacht, dann sind diese beiden Schaltflächen deaktiviert. Beim Anklicken der Schaltfläche ***Abbrechen*** wird das Fenster geschlossen, und alle Änderungen werden verworfen. Wird hingegen die Schaltfläche ***OK*** angeklickt, dann wird das Fenster geschlossen, und alle Änderungen werden gespeichert.

6.2.14.1 *Allgemein*

Auf der Registerkarte **Allgemein** lassen sich die folgenden Einstellungen vornehmen:

- ***Geteiltes Verzeichnis*** Gibt das Verzeichnis an, in dem die Datei ismxstartup.exe für die Bereitstellung von **IKARUS anti.virus** gespeichert ist.
  - **Schaltfläche Durchsuchen:** Öffnet ein Browserfenster zum Auswählen des geteilten Verzeichnisses.
  - Bitte beachten Sie, dass die benötigten Lese- und Schreibrechte gesetzt werden müssen (siehe Abschnitt 7)
- **Client-Update erzwingen:** Bereitstellung über *TCP* aktivieren bzw. deaktivieren.
- **Client-Update-Port erzwingen:** Erzwingt die Bereitstellung über den festgelegten TCP-Port.
- **Verwaltungsport:** Jener Port, den die Benutzeroberfläche des **IKARUS security.manager** zur Kommunikation mit dem **IKARUS security.manager-Server** einsetzt.
- **Automatisch Clients hinzufügen:** Legt fest, ob neue Clients im *LDAP* automatisch zum Verzeichnis hinzugefügt werden.

Über den Bereich **Leistungseinstellungen** lassen sich Einstellungen festlegen, die zu einer gesteigerten Performance führen können:

- **Maximale Anzahl gleichzeitiger Verbindungen**: Gibt an, wie viele gleichzeitige Verbindungen der **IKARUS security.manager** annimmt. Das betrifft Verbindungen zwischen **IKARUS security.manager** GUI und Server als auch Verbindungen zu **IKARUS anti.virus** Installationen. Diese Einstellung hat keinen Einfluss auf die Anzahl der verwaltbaren Clients sondern regelt nur deren Kommunikation mit dem **IKARUS security.manager**. 0 für unendlich viele gleichzeitige Verbindungen.
- **Maximale Anzahl gleichzeitiger Downloads**: Sollten keine Fileshares vorhanden sein, laden verwaltete Hosts mit IKARUS anti.virus Updates direkt vom IKARUS security.manager. Diese Einstellung legt fest, wie viele Hosts gleichzeitig Updates herunterladen dürfen. 0 für unendlich viele gleichzeitige Downloads.

© 2013 IKARUS Security Software GmbH

Im Bereich **Change Management** lassen sich die folgenden Optionen aktivieren bzw. deaktivieren:

- **Change Management gemäß IT-Infrastrukturbibliothek aktivieren:** Nachverfolgung von Änderungen aktivieren bzw. deaktivieren.
- **Auf Anmeldemaske um Kommentar ersuchen:** Bei erfolgter Aktivierung muss der Benutzer bei Anmeldeversuchen einen Kommentar eingeben.
- **Change Log für Servereinstellungen führen:** Bei erfolgter Aktivierung werden sämtliche Änderungen der Einstellungen protokolliert.
- **Nach ID für Request for Change (RfC) ID fragen:** Bei erfolgter Aktivierung muss der Benutzer bei Anmeldeversuchen eine RfC-ID eingeben.

Im Bereich **Verwendung von config-Dateien nach Drag and Drop** lassen sich die folgenden Einstellungen vornehmen:

- **Drag-and-Drop-Verhalten:** Bei erfolgter Aktivierung erhält der Benutzer eine Benachrichtigung darüber, was er nach Verschieben von Hosts in die manuelle Gruppe mit den config-Dateien tun soll.
- **Standardverhalten festlegen:** Falls dasselbe Verhalten in jedem einzelnen Fall angewendet werden soll, so legen Sie bitte fest, ob die Hosts ihre eigenen oder eine übergeordnete config-Datei benutzen sollen.

Signature Quality Assurance ist eine Funktion von **IKARUS anti.virus,** um die Informationen über Virenfunde anonymisiert an IKARUS zur besseren Auswertung zu senden. Ist SigQA aktiviert, nehmen alle verwalteten Hosts daran teil.

Debug Logging aktiviert erweitertes, serverseitiges Logging. Dies kann in Supportfällen hilfreich sein.

© 2013 IKARUS Security Software GmbH

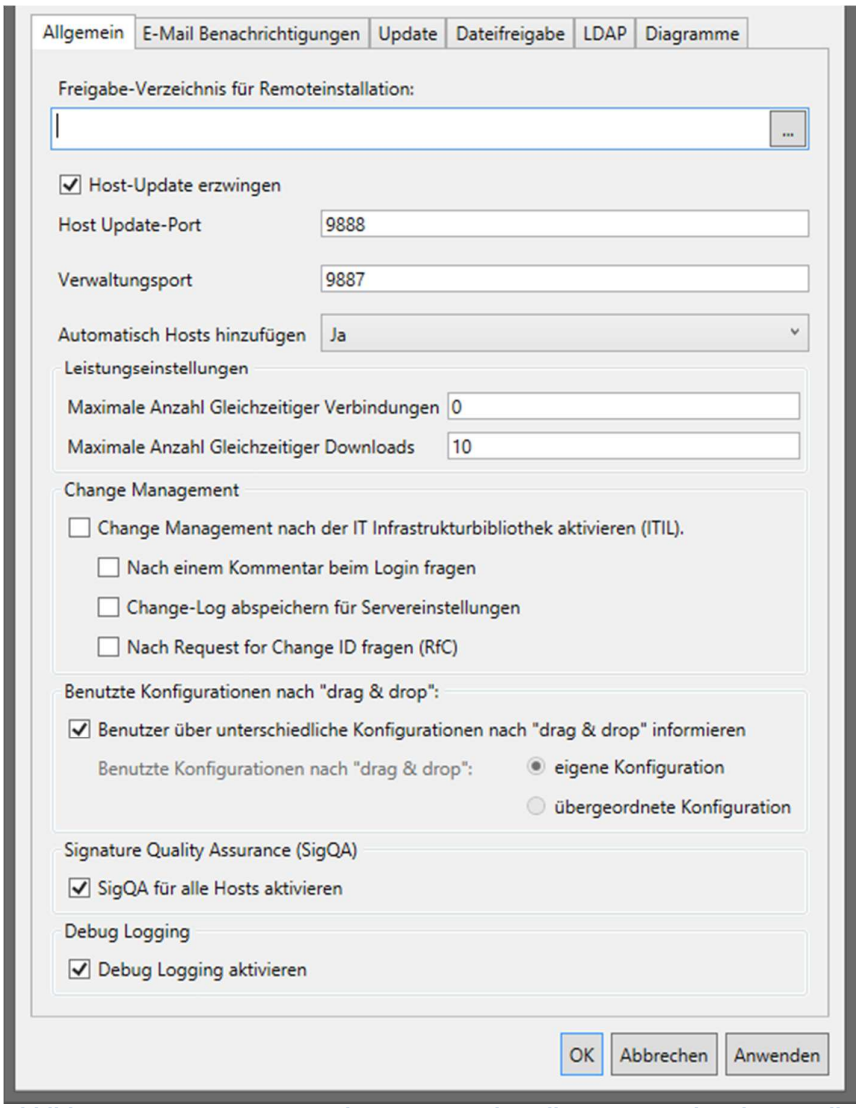


Abbildung 6-43: „IKARUS security.manager-Einstellungen“, Registerkarte „Allgemein“

© 2013 IKARUS Security Software GmbH

6.2.14.2 *E-Mail-Benachrichtigungen*

Auf der Registerkarte **E-Mail** lassen sich die folgenden Einstellungen vornehmen:

- **E-Mail Berichte aktivieren:** Aktiviert bzw. deaktiviert E-Mail-Berichte.
- **Mailserver:** Legt jenen Mailserver fest, über welchen die Berichte gesendet werden.
- **Absender:**. Die Adresse, von der aus die Berichte versendet werden.
- **Authentifizierung aktivieren:** Aktiviert bzw. deaktiviert die Benutzerauthentifizierung auf dem Mailserver.
- **Benutzername:** Der zur Authentifizierung auf dem Mailserver verwendete Benutzername.
- **Passwort:** Das zur Authentifizierung auf dem Mailserver verwendete Passwort.
- **Verfügbare Berichte:** Listet alle vorhandenen Berichte auf.
- **Neuen Bericht hinzufügen:** Öffnet das Fenster **IKARUS security.manager-Berichte**, siehe Abschnitt 6.2.14.3.

Abbildung 6-44: „IKARUS security.manager-Einstellungen“, Registerkarte „E-Mail-Benachrichtigungen“

6.2.14.3 ***IKARUS security.manager*-Berichte**

Im Bericht-Dialog können folgende Einstellungen zur Konfiguration eines E-Mail Berichts getätigt werden:

- **Berichtname:** Setzt den Namen des Berichts.
- **Bericht aktivieren:** Aktiviert oder deaktiviert das Versenden dieses Berichts.
- **Bericht-Art:** Gibt die Art des Berichts an, folgende Arten sind verfügbar:
  - **Bericht beim Auftreten eines Virus**
  - **Bericht beim automatischen Hinzufügen von Hosts**

© 2013 IKARUS Security Software GmbH

  - **Tagesbericht:** Ein Bericht wird an allen ausgewählten Wochentagen gesendet.
  - **ISM Server Startup Bericht:** Bericht wird bei jedem Start des IKARUS security.manager Servers gesendet.
  - **Intervall Report:** Bericht wird immer zu einer bestimmten Zeit gesendet.
  - **License expires Report:** Bericht wird einige Tage vor Ablauf der Lizenz gesendet.
- **Geplante Zeit:** Setzt die Zeit, zu der der Bericht gesendet wird.
- **Tagesmaske:** Setzt die Wochentage, an denen der Bericht gesendet wird.
- **Virenbericht aktivieren:** Bericht soll Virenbericht enthalten.
- **Versionsbericht aktivieren:** Bericht soll Versionsbericht enthalten.
- **Hostbericht aktivieren:** Bericht soll Hostbericht enthalten.
- **Serverbericht aktivieren:** Bericht soll Serverbericht enthalten.
- **Hinzufügen:** Berichtsempfänger hinzufügen.
- **Empfänger:** Liste aller Empfänger.

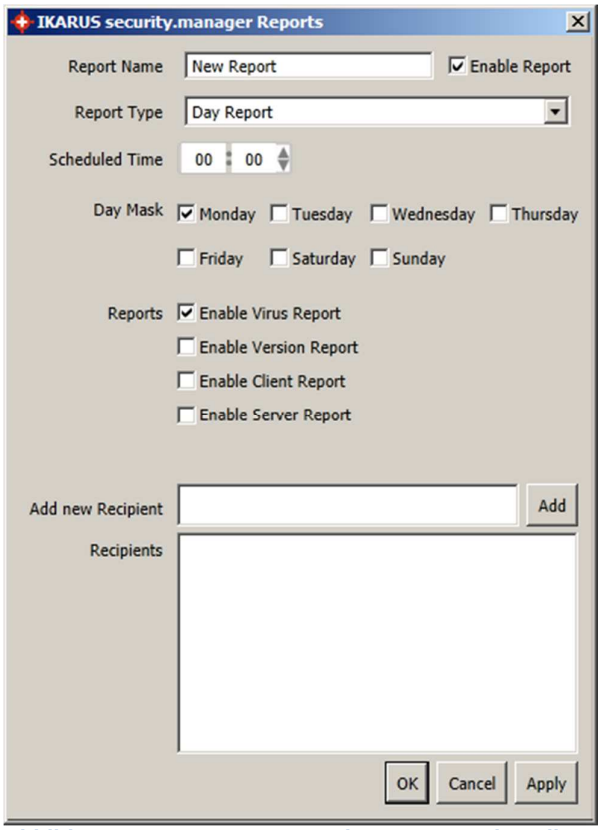


Abbildung 6-45: „IKARUS security.manager-Einstellungen“, Registerkarte „Berichte“

© 2013 IKARUS Security Software GmbH

6.2.14.4 *Update*

Auf der Registerkarte **Update** lassen sich folgende Einstellungen vornehmen:

- Stilles Update des IKARUS security.manager-Servers: Aktiviert die automatische Aktualisierung des IKARUS security.manager-Servers.
- ***Proxyserver*:** Legt jenen Proxyserver fest, über den der **IKARUS security.manager-Server** die Updates abruft.
- **Proxyport:** Legt den Proxyport fest, über welchen die Verbindung hergestellt wird.
- **Benutzername:** Legt den Benutzernamen fest, der gegebenenfalls für die Authentifizierung auf dem Proxyserver benötigt wird.
- **Passwort:** Legt das Passwort fest, das gegebenenfalls für die Authentifizierung auf dem Proxyserver benötigt wird.

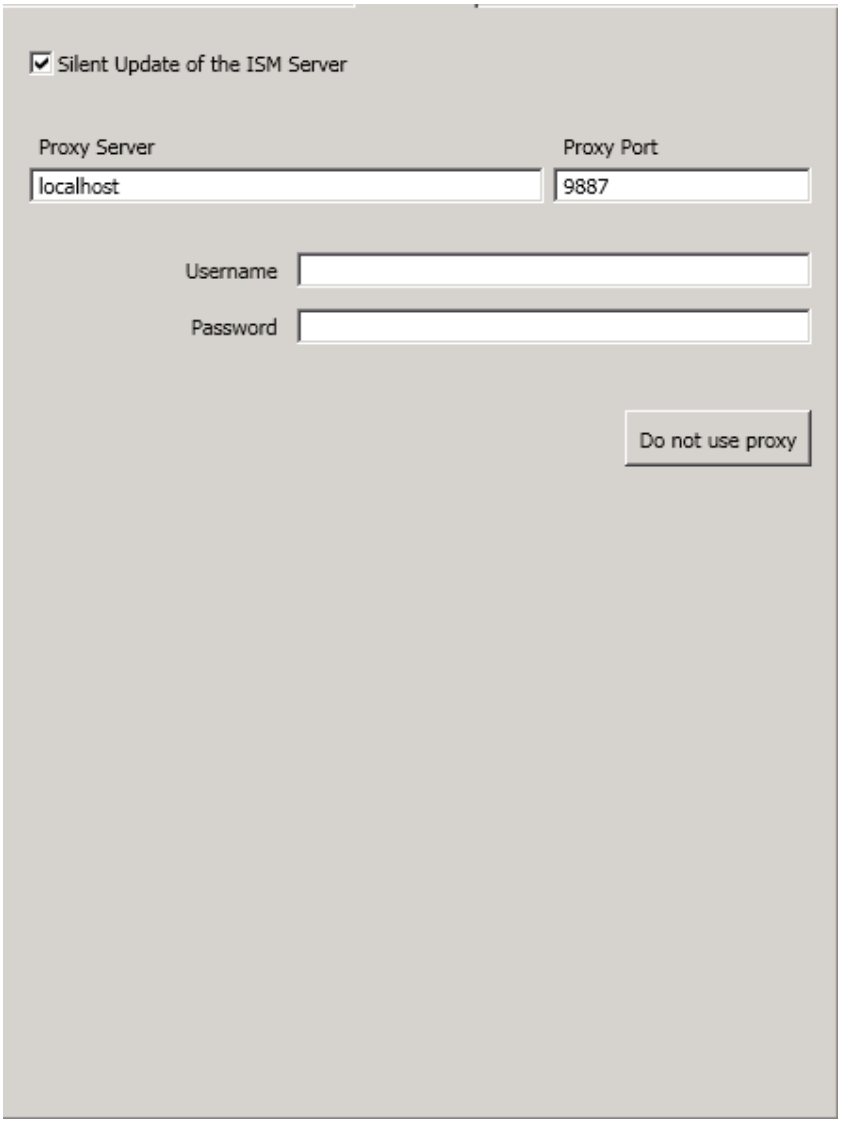


Abbildung 6-46: „IKARUS security.manager-Einstellungen“, Registerkarte „Update“

© 2013 IKARUS Security Software GmbH

6.2.14.5 *Fileshare*

Zur Vermeidung von Engpässen bei den Systemressourcen sollten *Fileshares* eingesetzt werden. Dazu müssen Administratoren zuerst *Fileshares* festlegen, die zusammen mit dem **IKARUS security.manager** eingesetzt werden sollen. Bitte beachten Sie, dass der **IKARUS security.manager-Server Lese- und Schreibrechte benötigt**, um die Daten stets auf dem neuesten Stand zu halten. In Abbildung 6-47 sehen Sie die Registerkarte *Fileshare*.

Auf der Liste der Registerkarte **Fileshare** werden folgende Informationen angezeigt:

- **Online/Offline:** Ein Fileshare wird auf "online" gestellt, wenn sämtliche Dateien verfügbar und aktuell sind.
- **Randomisierte Datenbasis:** Ein Fileshare, bei dem es sich um eine randomisierte Datenbasis handelt, wird dabei nach Zufallsprinzip einem Host zugeordnet, der gerade ein Update benötigt.
- **Fileshare-Liste:** Enthält sämtliche aktiven bzw. inaktiven Fileshares.

Auf der Registerkarte Fileshare können die beiden folgenden Aktionen durchgeführt werden:

- **Rollout starten:** Beim Hinzufügen neuer Fileshares kann es sein, dass die Benutzer sofort mit einem Rollout der Dateien beginnen wollen.
- **Fileshare hinzufügen:** Hinzufügen eines neuen Fileshare. Fileshares werden auf "online" gestellt, sobald sämtliche Dateien im Zuge des Rollout-Vorgangs kopiert wurden.

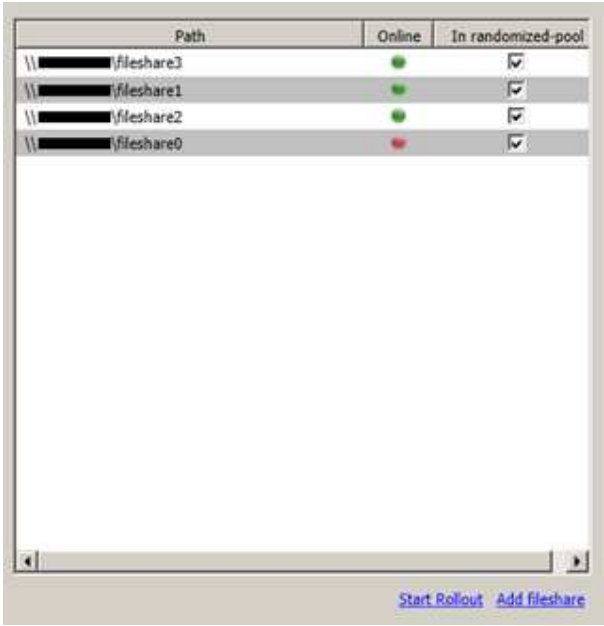


Abbildung 6-47 UI –Einstellungen IKARUS security.manager, "Fileshare"

Der IKARUS security.manager-Server prüft **einmal pro Minute**, ob ein *Fileshare* zur Verfügung steht. Der jeweils aktuelle Zustand wird durch ● (*Fileshare* ist online) oder ● (*Fileshare* ist offline) dargestellt (siehe Abbildung 6-47, zweite Spalte). Ein *Fileshare* ist dann verfügbar, wenn sämtliche Dateien **vorhanden und aktuell** sind. Zu beachten ist, dass Fileshares auf 260 Zeichen beschränkt sind.

© 2013 IKARUS Security Software GmbH

Außerdem prüft der **IKARUS security.manager-Server** alle **20 Minuten**, ob Updates verfügbar sind und in die festgelegten *Fileshares* kopiert werden müssen. Der Rollout-Prozess der Aktualisierungsdateien kann auch **manuell mithilfe von "Rollout starten"** initiiert werden (siehe Abbildung 6-47). Ein **einmal pro Tag** eingeleiteter Löschvorgang entfernt alte Dateien, um so die Datenmenge so gering wie möglich zu halten.

Fileshares werden über die **Eigenschaftsseite im Update-Bereich** (siehe Abschnitt 6.2.6) entsprechenden Hosts bzw. Gruppen zugewiesen.

6.2.14.6 *LDAP*

Auf der *LDAP*-Registerkarte können die Benutzer die *LDAP*-Einstellungen durch Verändern der folgenden Einstellungen konfigurieren:

- **Domäne automatisch erkennen:** Versucht die Domäne automatisch zu erkennen
- **Servername:** Name des Domänencontrollers (siehe Abschnitt 10.2)
- **Typ:** *LDAP* -Typ (siehe Abschnitt 10.2)
- **Eigenschaften:** Stellt Eigenschaften auf "Lesen" (siehe Abschnitt 10.2)
- **Suchpfad:** Legt die zu scannende Domäne fest (siehe Abschnitt 10.2)
- **Filter:** Legt jene Kriterien fest, die zur Verarbeitung der festgelegten Eigenschaft verwendet werden sollen (siehe Abschnitt 10.2)
- **Authentifizierungsmethode:** Methode zur Authentifizierung auf dem Domänencontroller (siehe Abschnitt 10.2)
- **Benutzername:** Legt den Benutzernamen für die *LDAP* -Verbindung fest (siehe Abschnitt 10.2)
- **Passwort:** Legt das Passwort für die *LDAP* -Verbindung fest (siehe Abschnitt 10.2)
- **Ausnahmen:** Überblick über die festgelegten Ausnahmen
- **Ausnahmen hinzufügen:** Fügt einen neuen Host hinzu, der nicht im Verzeichnis angeführt ist
- **Testen der LDAP-Einstellungen:** Hier wird getestet, ob unter Berücksichtigung der angegebenen Parameter ein *LDAP* aufgefunden werden kann.

© 2013 IKARUS Security Software GmbH

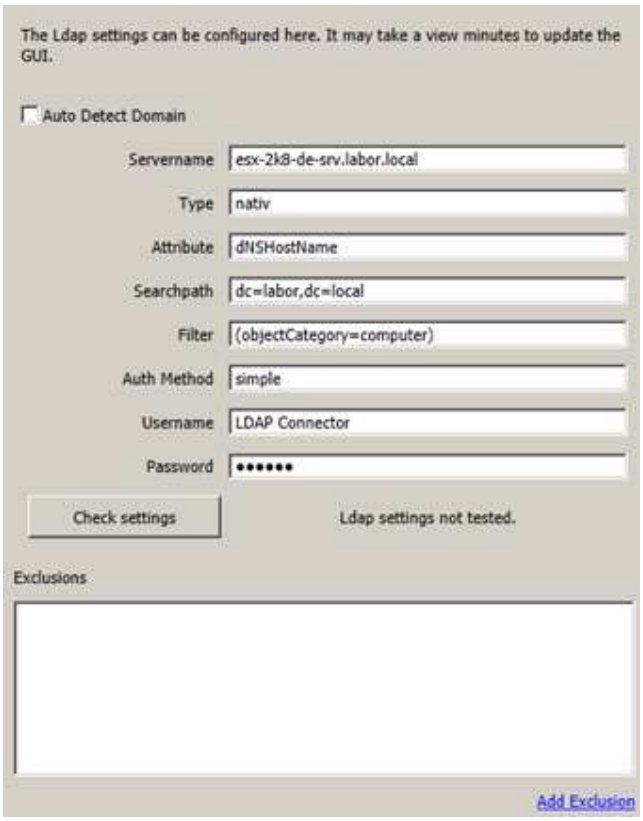


Abbildung 6-48 UI – Einstellungen IKARUS security.manager – LDAP

LDAPs lassen sich mithilfe des in Abbildung 6-48 dargestellten Dialogfelds einsetzen; davor wurden *LDAPs* in der config-Datei konfiguriert. Wenn sich in der config-Datei ein <ldap>-Abschnitt befindet, **wird dieser Abschnitt vom IKARUS security.manager-Server automatisch gelesen und eingestellt**. Danach **wird** der <ldap>-Abschnitt aus der config-Datei **gelöscht**.

Für die Festlegung eines *LDAP* gibt es daher **zwei verschiedene Methoden**:

- Benutzen Sie die *LDAP*-Registerkarte in den **Einstellungen des IKARUS security.manager**
- Fügen Sie den <ldap>-Abschnitt zur **config-Datei** hinzu

Weitere Informationen zur config-Datei und den *LDAP*-Parametern finden Sie in Kapitel 9 sowie in Abschnitt 10.2.

6.2.14.7 *Diagramme*

Auf der Registerkarte **Diagramme** lassen sich das Aussehen der Standarddiagramme sowie der dazugehörige Beschreibungstext abändern (siehe Abbildung 6-49).

© 2013 IKARUS Security Software GmbH

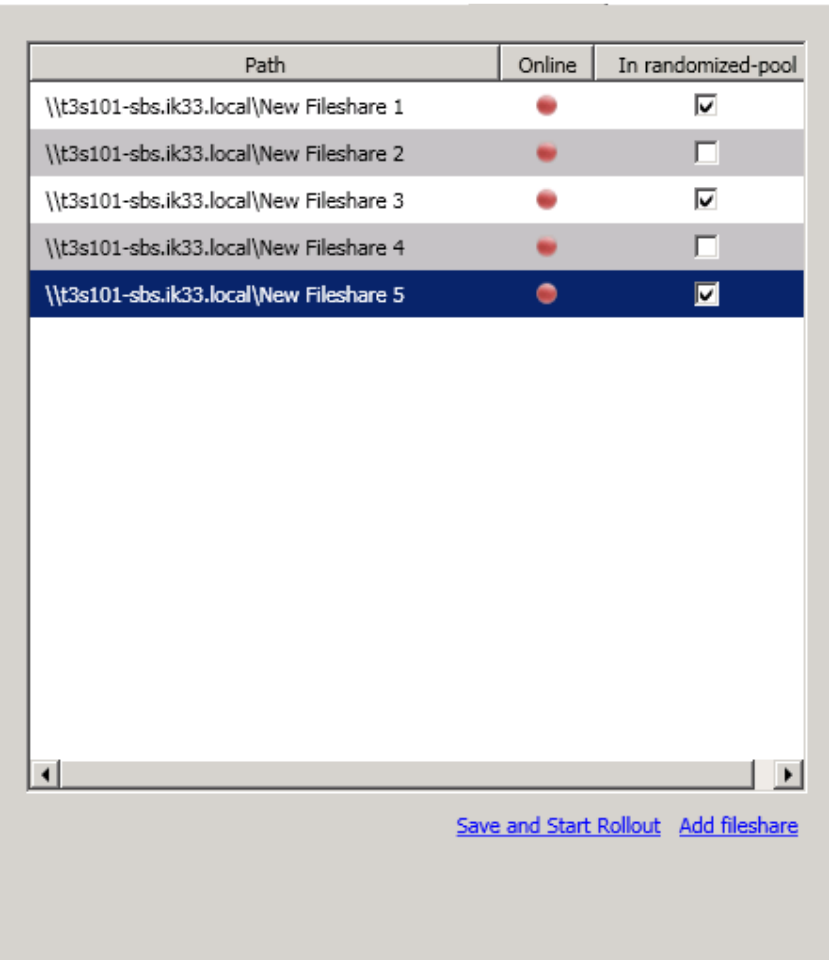


Abbildung 6-49 Diagrammoptionen

Bereich mit der Diagrammliste:
Im oberen Bereich des Dialogfelds sind die 5 Standarddiagramme aufgelistet.

- Die **Reihenfolge** der Diagramme lässt sich mithilfe der Pfeiltasten **ändern**.
- Mithilfe des aktivierten Kontrollkästchens lassen sich **Diagramme** sowohl auf der Diagrammseite als auch in der PDF-Datei (siehe Abschnitt 6.2.11) **verbergen**.
- Bei Auswahl des **Diagrammtyps** "Tortendiagramm" kann die ermittelte Anzahl durch Anklicken des Kontrollkästchens "Gezählte Anzahl anzeigen" neben den Prozentwerten innerhalb des Diagramms angezeigt werden.

Einstellungen für diesen Bereich:
Die Einstellungen sind in 3 Teile gegliedert und sind von jenem Diagramm abhängig, welches in der Diagrammliste oben ausgewählt wurde.

Im Bereich **Hinweistext anzeigen** kann festgelegt werden, wo die Bildunterschrift des Diagramms platziert werden soll (oben rechts, rechts, unten rechts), oder ob überhaupt eine Bildunterschrift abgebildet werden soll

Im Bereich **Formateigenschaften** kann der Diagrammtyp (Torten- oder Balkendiagramm) ausgewählt und dessen Breite und Höhe festgelegt werden, um das jeweilige Diagramm optimal der Auflösung Ihres Bildschirms anzupassen. Die Mindesthöhe und -breite der Diagramme beträgt 500 Pixel.

© 2013 IKARUS Security Software GmbH

Im Bereich **Zusätzlicher Text** können Sie Ihre eigenen, individuell erstellten Beschreibungen hinzufügen. Diese Beschreibungen werden sowohl im Bericht als auch auf der Diagrammseite angezeigt.

PDF-Bericht:
Beim Anklicken des von **PDF-Einstellungen** unten links öffnet sich ein Dialogfeld, in dem Sie die Standardkopf- und -fußzeile des Berichts abändern und Ihre **eigene, individuell erstellte Kopf- und Fußzeile** einfügen können (siehe Abbildung 6-50). Ebenso möglich ist ein Zurücksetzen auf die Standardkopf- und -fußzeile. Kopf- und Fußzeile lassen sich auch deaktivieren und werden danach nicht im Bericht angezeigt. Diese Einstellungen wirken sich lediglich auf das Aussehen des **PDF-Berichts** aus.

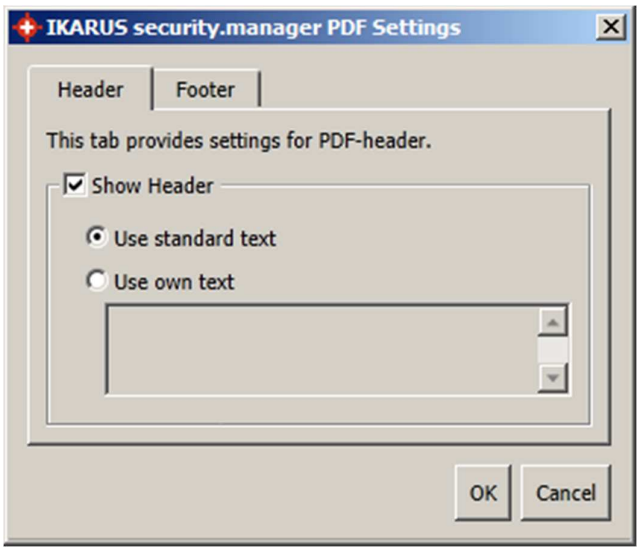


Abbildung 6-50 Einstellungen PDF-Bericht

© 2013 IKARUS Security Software GmbH

6.2.15 Dialog „Host-Einträge aus der Datenbank löschen“

Dieser Dialog sollte nur verwendet werden, wenn Hosts **manuell aus dem aktiven Verzeichnis gelöscht wurden**. Diese gelöschten Hosts können möglicherweise noch in der Datenbank aufscheinen und über dieses Dialogfeld unwiderruflich aus dieser gelöscht werden. **Bitte beachten Sie, dass dieser Löschvorgang nicht rückgängig gemacht werden kann!**

Auf der linken Seite des Dialogfensters werden sämtliche ungenutzten Hosts angezeigt. Dabei handelt es sich um Hosts, die sich noch immer in der Datenbank befinden und verwaltet werden, jedoch nicht mehr in Ihrem *Aktiven Verzeichnis* oder in Ihrer manuellen Gruppe aufscheinen. Ein solcher Fall kann vorkommen, weil der **IKARUS security.manager** Hosts nicht automatisch vom Server löscht, sobald diese nicht mehr im *Aktiven Verzeichnis* zur Verfügung stehen, da der Server nicht in der Lage ist, das Benutzerverhalten vorwegzunehmen.

IKARUS security.manager-Administratoren müssen diese Hosts durch Verschieben von der linken Liste mit der Bezeichnung **Aus dem aktiven Verzeichnis gelöschte Hosts** in die rechte mit der Bezeichnung **Zu löschende Hosts** manuell entfernen. Zum Verschieben von Hosts zwischen den beiden Listen stehen zwischen den Listen 4 Schaltflächen zur Verfügung:

- **Alle Hosts auswählen:** Alle Hosts werden zum Entfernen aus der Hostliste festgelegt
- **Einen Host auswählen:** Der ausgewählte Host wird zum Entfernen aus der Hostliste festgelegt
- **Auswahl des Hosts rückgängig machen:** Der ausgewählte Host wird von der Liste der zu entfernenden Hosts genommen
- **Auswahl aller Hosts rückgängig machen:** Alle Hosts werden von der Liste der zu entfernenden Hosts genommen

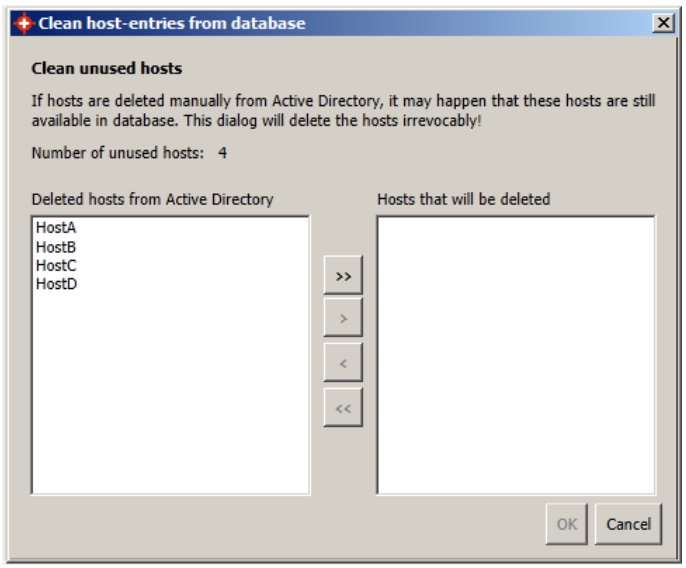


Abbildung 6-51 UI – Host-Einträge aus der Datenbank entfernen

© 2013 IKARUS Security Software GmbH

Nach Entfernen ungenutzter Hosts aus der Datenbank kann es vorkommen, dass Lizenzen, die zuvor den ausgewählten Hosts zugeordnet waren, wieder frei werden. Dieser Dialog lässt sich unter **Werkzeuge →Host-Einträge aus der Datenbank entfernen** aufrufen.

© 2013 IKARUS Security Software GmbH

6.2.16 Management-Modus

Über diesen Menüpunkt erhalten Sie Zugriff auf all jene Optionen, die den Management-Modus des **IKARUS security.managers** betreffen. Sie bekommen hier einen Überblick über Ihre **IKARUS security.manager** Instanzen und können diese bearbeiten, löschen und neue hinzufügen. Des Weiteren können Sie über dieses Menü die Einstellungen Ihrer **IKARUS security.manager** Instanzen in eine passwortgeschützte Datei exportieren und das Passwort für die Konfigurationsdatei des Management Modus ändern.

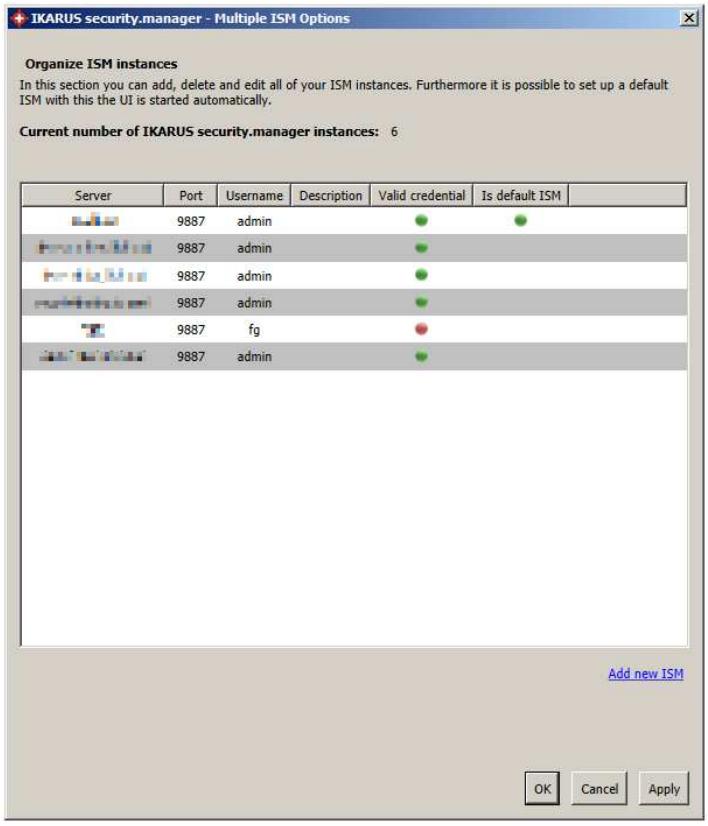
Beachten Sie, dass dieses Menü im **Einzel-Modus nicht verfügbar ist!**

6.2.16.1 *Der Menüpunkt „Optionen“*

Der Optionen Dialog ist über das Hauptmenü unter dem Punkt **“Optionen”** zu finden.

Abbildung 6-52 : UI - Menü "Management", Menüpunkt "Konfigurationsdatei exportieren"

Der Dialog bietet eine Übersicht über Ihre **IKARUS security.manager** Instanzen. In der Liste werden diese mit Servername, Port, Username und Beschreibung dargestellt. Außerdem sehen Sie, ob eine Instanz gültige Verbindungsdaten hat und ob sie als Standard-Instanz eingerichtet ist.



© 2013 IKARUS Security Software GmbH

Abbildung 6-53 : UI – Optionen Dialog

Sie können die vorhandenen Instanzen bearbeiten, löschen und als Standard Instanz setzen. Alle Operationen sind vom Kontextmenü aus aufrufbar:

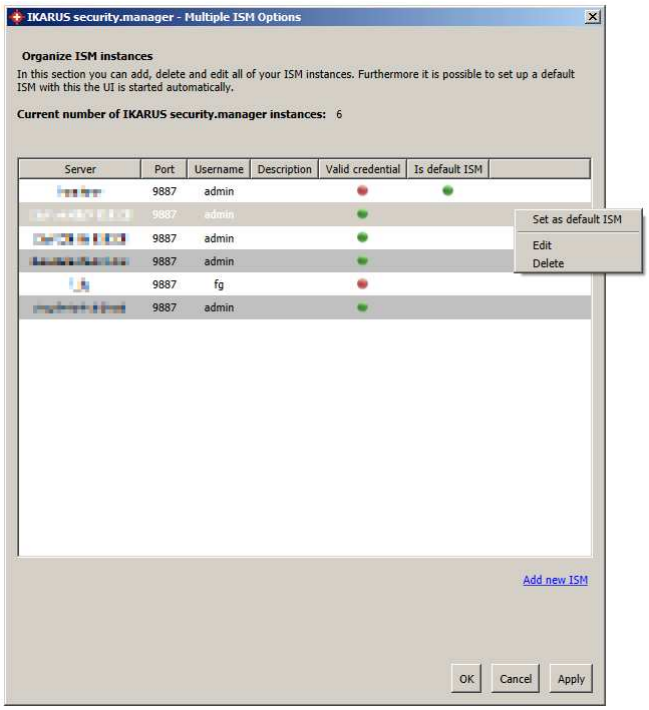


Abbildung 6-54 : UI – Kontextmenü im Optionen Dialog

„Als Standard ISM setzen“ bewirkt, dass bei einem Programmneustart die Verbindung automatisch zu dieser **IKARUS security.manager** Instanz hergestellt wird. Es muss immer eine Standard-Instanz geben. Sie können diese nicht löschen.

Durch einen Klick auf „Löschen“ wird die ausgewählte Instanz aus Ihrer Liste gelöscht. Beachten Sie, dass Sie die **IKARUS security.manager** Instanz, zu der Sie aktuell verbunden sind, und die Standard-Instanz nicht löschen können! Das Löschen von Instanzen ist auch möglich, indem Sie eine Instanz auswählen und anschließend die Entfernen-Taste Ihrer Tastatur drücken.

6.2.16.1.1 IKARUS security.manager-Server editieren

Wenn Sie im Kontextmenü einer **IKARUS security.manager** Instanz auf „Bearbeiten“ klicken, gelangen Sie zum Bearbeiten-Dialog. Sie haben hier die Möglichkeit Servername, Port, Username, Passwort und die Beschreibung zu verändern.

Alternativ können Sie doppelt auf eine **IKARUS security.manager** Instanz in der Liste klicken, dies öffnet ebenfalls den Bearbeiten-Dialog.

© 2013 IKARUS Security Software GmbH

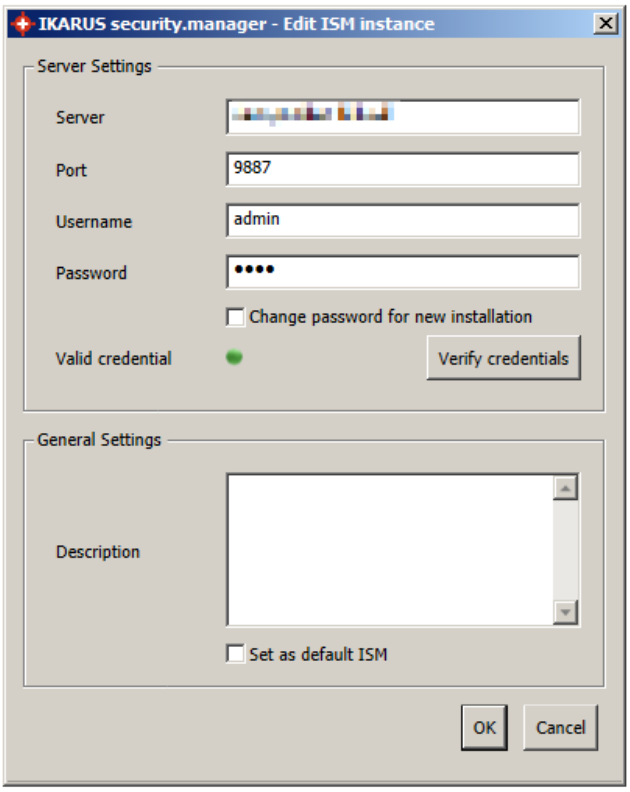


Abbildung 6-55 : UI – Bearbeiten Dialog

Sie werden vom Programm auf ungültige Eingaben aufmerksam gemacht. Eine Bestätigung der Daten ist nur möglich, wenn alle Eingaben als gültig erkannt werden. Die Portnummer muss beispielsweise in einem bestimmten Zahlenbereich liegen, um diese Instanz erfolgreich erstellen zu können.

© 2013 IKARUS Security Software GmbH

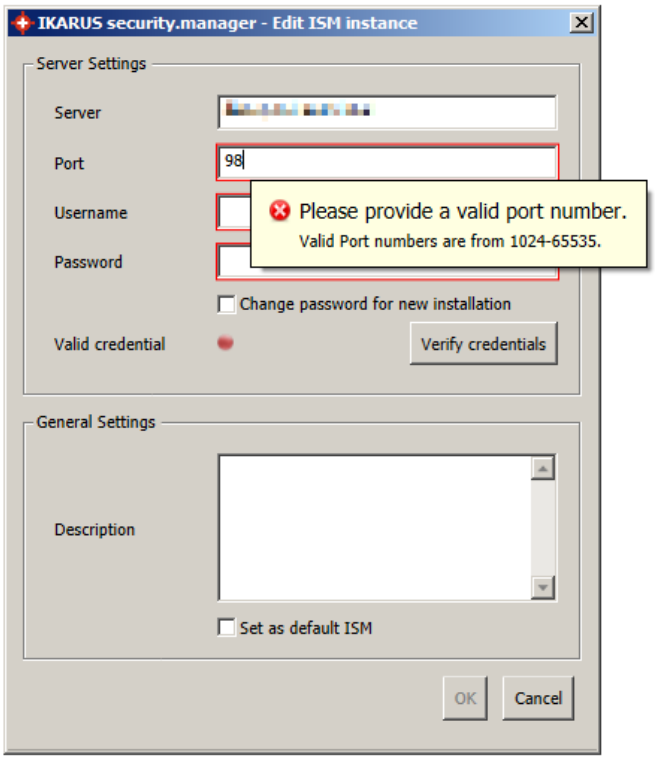


Abbildung 6-56 : UI – Bearbeiten Dialog, Eingabe ungültiger Daten

Aktivieren Sie die Option „Passwort für eine neue Installation ändern“, können Sie das Passwort der **IKARUS security.manager** Instanz verändern. Das ist allerdings nur nach einer neuen Installation möglich.

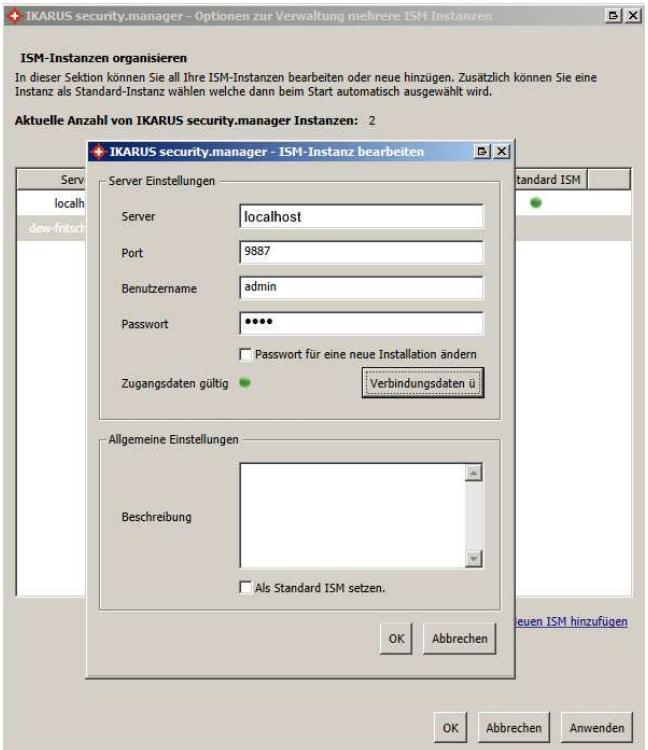


Abbildung 6-57 : UI – Bearbeiten Dialog, Passwort für eine neue Installation ändern

© 2013 IKARUS Security Software GmbH

Sie müssen in beide Passwort-Felder denselben Wert eingeben. Durch Klick auf „Passwort setzen“ wird überprüft, ob die Passwortänderung möglich ist. Wenn ja, wird das Passwort der **IKARUS security.manager** Instanz neu gesetzt.

Durch Klick auf den Button “Verbindungsdaten überprüfen” überprüft das Programm die Richtigkeit der eingegebenen Daten. Sie werden über das Ergebnis der Überprüfung durch ein Meldungsfenster sowie durch den Statusindikator links vom Button informiert. Dieser ist grün, wenn der Verbindungsaufbau erfolgreich war, oder rot, wenn die Testverbindung fehlgeschlagen ist.

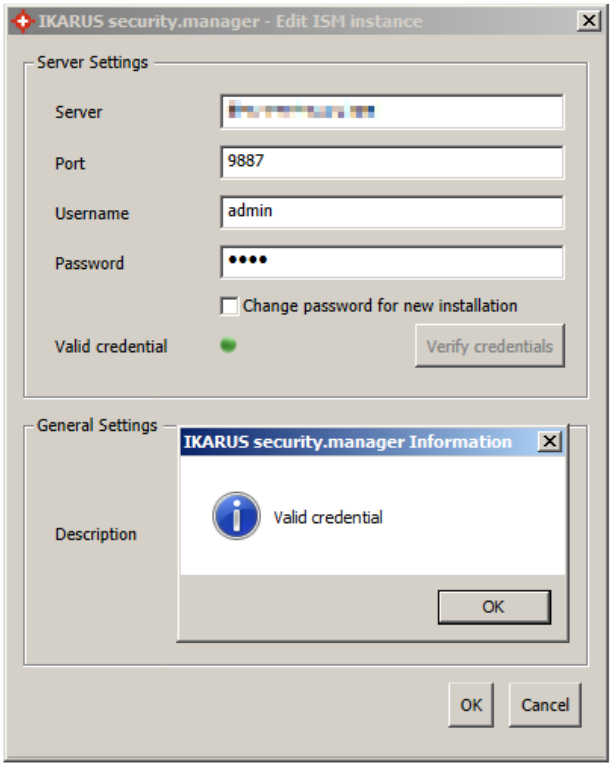


Abbildung 6-58 : UI – Bearbeiten Dialog, Überprüfung der Zugangsdaten

Mit der Checkbox am unteren Rand des Dialogs legen Sie fest, ob die Instanz Ihre Standard Instanz ist. Sie werden bei jedem Programmneustart automatisch zur Standard Instanz verbunden. Beachten Sie, dass es immer eine solche Standard Instanz geben muss, gegebenenfalls werden Sie vom Programm aufgefordert, diese Option zu setzen.

Wenn Sie alle benötigten Felder ausgefüllt haben und die eingegebenen Daten gültig sind, können Sie den Bearbeiten-Dialog mit einem Klick auf “OK” schließen.

6.2.16.1.2 IKARUS security.manager-Server hinzufügen

Im Optionen Dialog ist es außerdem möglich, neue Instanzen hinzuzufügen. Sie können dies über den “Instanz hinzufügen” Link unter der Liste machen. Ein Klick darauf öffnet den auf den vorherigen Seiten beschriebenen Bearbeiten-Dialog, natürlich sind

© 2013 IKARUS Security Software GmbH

noch keine Felder ausgefüllt – Sie müssen erst alle erforderlichen Informationen angeben.

Beachten Sie, dass Änderungen an den **IKARUS security.manager** Instanzen erst durch Klick auf “Übernehmen” bzw. “OK” dauerhaft übernommen werden.

6.2.16.2 *Der Menüpunkt „Konfigurationsdatei exportieren“*

Über den Dialog „Konfigurationsdatei exportieren” ist es möglich, die Einstellungen der einzelnen **IKARUS security.manager**-Instanzen verschlüsselt eine neue Konfigurationsdatei zu schreiben. Diese Datei kann dann nach Belieben weitergegeben werden. Sie können den Dialog über das Menü *Management* → *Konfigurationsdatei exportieren* aufrufen.

Abbildung 6-59: UI - Menü "Management", Menüpunkt "Konfigurationsdatei exportieren"

Zu beachten ist, dass das Menü „Management“ im Einzel-Modus nicht verfügbar ist!

Der Dialog zeigt eine Liste mit allen **IKARUS security.manager** -Instanzen sowie deren Kerninformationen. Sie können mithilfe der Checkboxen am linken Rand der Liste auswählen, ob alle Instanzen oder nur bestimmte exportiert werden sollen.

© 2013 IKARUS Security Software GmbH

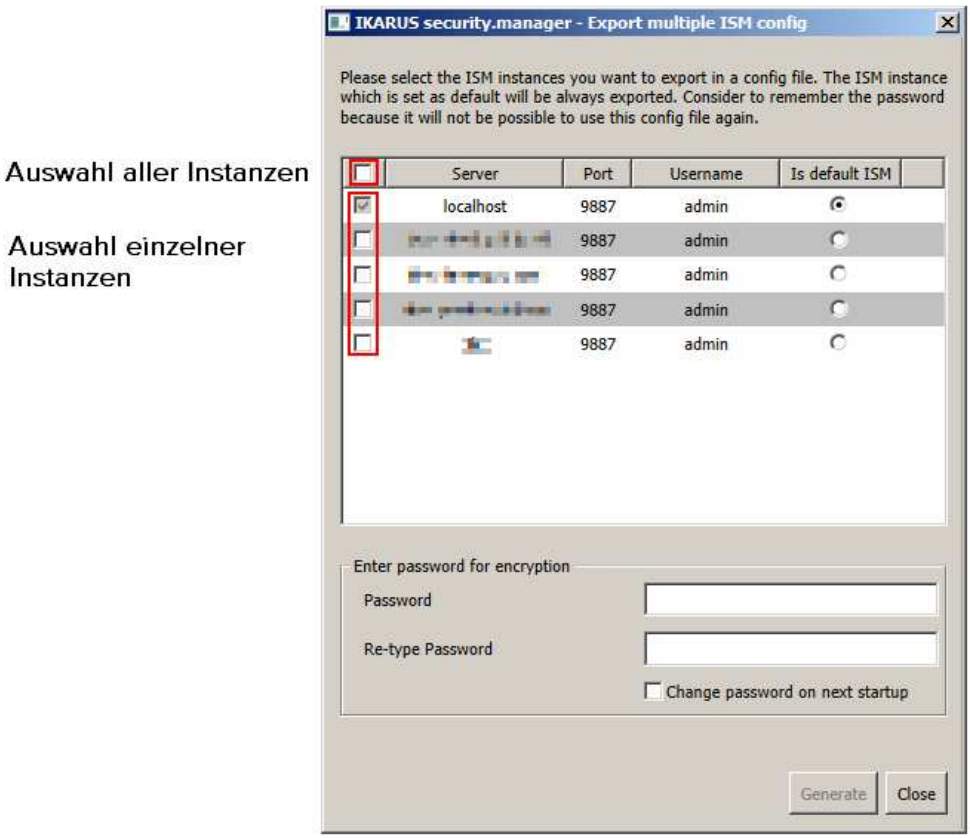

Auswahl aller Instanzen
Auswahl einzelner Instanzen
IKARUS security.manager - Export multiple ISM config
Please select the ISM instances you want to export in a config file. The ISM instance which is set as default will be always exported. Consider to remember the password because it will not be possible to use this config file again.
Server
Port
Username
Is default ISM
localhost
9887
admin
Enter password for encryption
Password
Re-type Password
Change password on next startup
Generate
Close

Abbildung 6-60: UI Dialog "Konfigurationsdatei exportieren“ – Auswahl der zu exportierenden ISM Instanzen

Aus Sicherheitsgründen ist vor dem Exportieren der Datei die Angabe eines Passworts notwendig, mit dem die Datei verschlüsselt wird. Sie müssen dieses über die zwei Textfelder unter der Liste angeben, wobei die Eingabe jeweils ident sein muss.

Achtung: Das Passwort muss mindestens 4 Zeichen lang sein und Sie müssen in beiden Textfeldern denselben Wert eingeben. Erst wenn diese Bedingungen erfüllt sind, können Sie die Daten exportieren.

© 2013 IKARUS Security Software GmbH

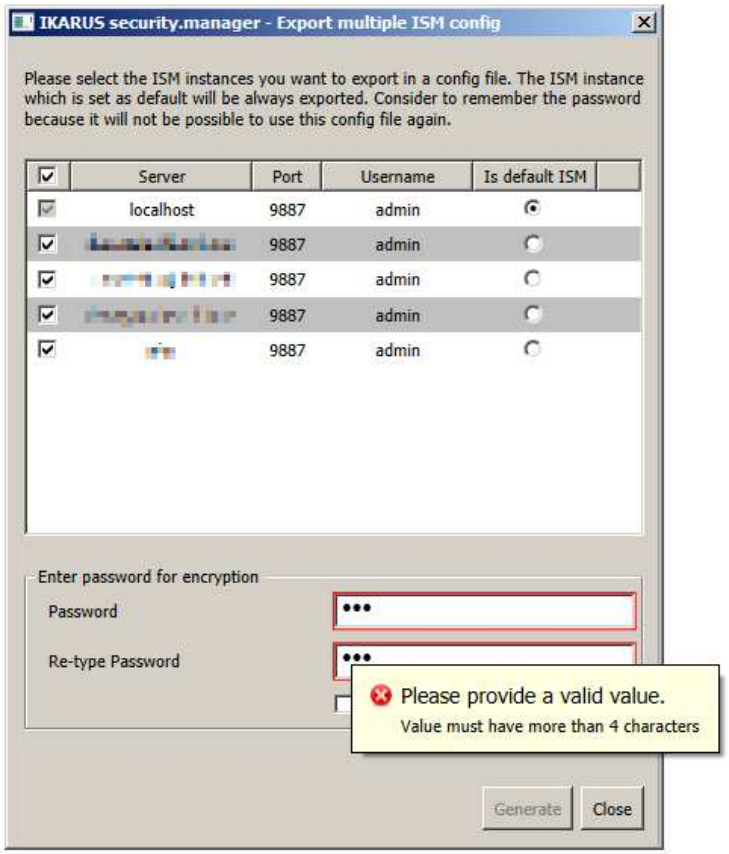


Abbildung 6-61: UI - Dialog "Konfigurationsdatei exportieren“ – Fehlermeldung bei ungültigem Passwort

Wenn Sie „Passwort muss beim nächsten Start geändert werden“ anhaken wird der Benutzer, der Ihre exportierte Datei verwenden will, beim ersten Programmstart mit Ihrer Konfigurationsdatei aufgefordert, das Passwort für die Verschlüsselung der Datei neu zu setzen. Andernfalls wird dafür der von Ihnen gesetzte Wert verwendet.

© 2013 IKARUS Security Software GmbH

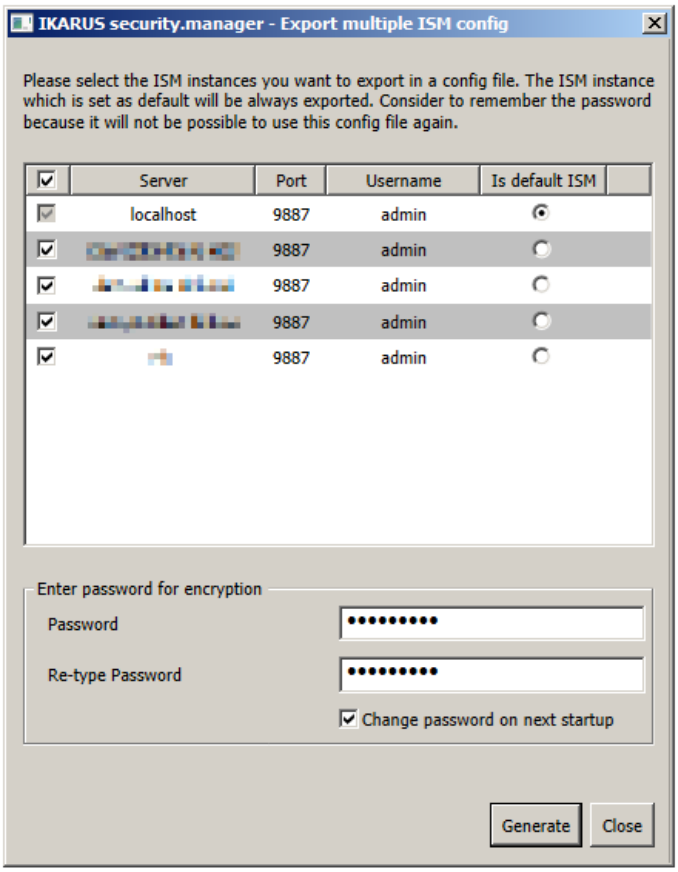

IKARUS security.manager - Export multiple ISM config
Please select the ISM instances you want to export in a config file. The ISM instance which is set as default will be always exported. Consider to remember the password because it will not be possible to use this config file again.
Server
Port
Username
Is default ISM
localhost 9887 admin
9887 admin
9887 admin
9887 admin
9887 admin
Enter password for encryption
Password
Re-type Password
Change password on next startup
Generate
Close

Abbildung 6-62: UI - Dialog "Konfigurationsdatei exportieren“ – Gültiges Passwort

Sie können die ausgewählten **IKARUS security.manager** Instanzen nun durch einen Klick auf „Generieren“ den Export starten. Im Folgedialog werden Sie noch aufgefordert, den Speicherpfad sowie einen Dateinamen anzugeben.

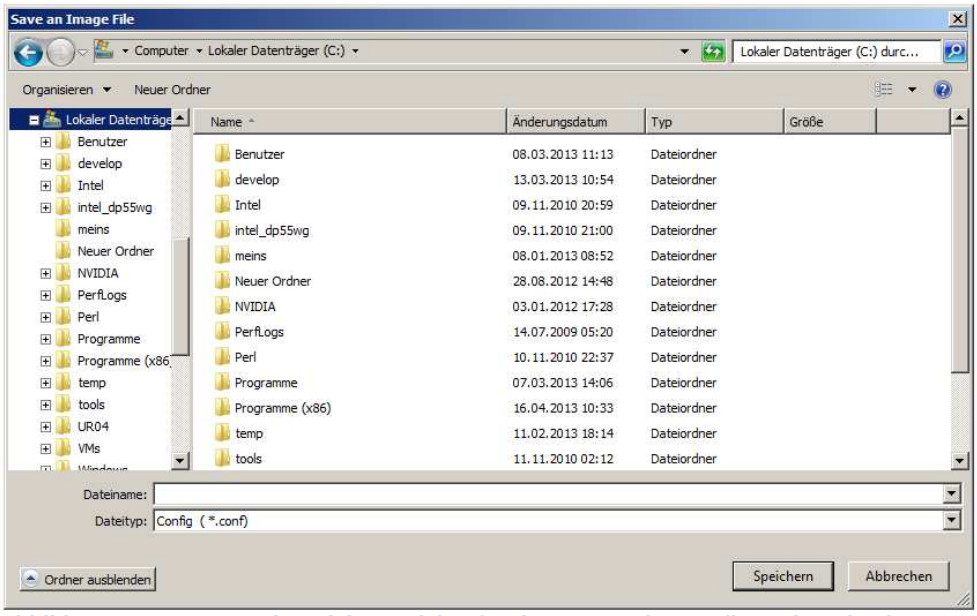


Abbildung 6-63: UI – Datei-Speichern Dialog für den Export der Konfigurationsdatei

© 2013 IKARUS Security Software GmbH

Ein Klick auf „Speichern“ speichert die Informationen verschlüsselt in der neuen Datei ab.

6.2.16.3 *Der Menüpunkt „Ändern Sie das Passwort für den Management-Modus“*

Um das Passwort für die Anmeldung im Management-Modus zu ändern kann der Dialog in genutzt werden. Dieser ist unter dem Menüpunkt Management verfügbar.

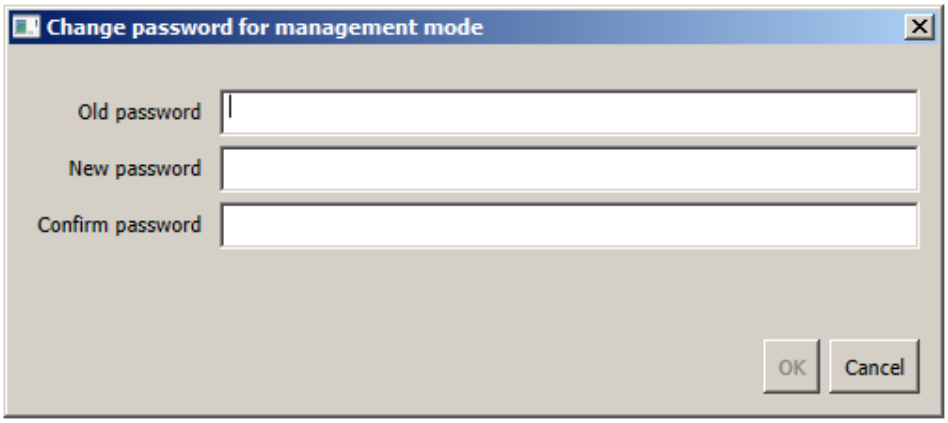


Abbildung 6-64: UI – Ändern Sie das Passwort fur den Management-Modus

Zu beachten gilt jedoch, dass Passwortänderungen im Management-Modus keine Auswirkungen auf die Passwörter der eingetragenen **IKARUS security.manager-Server** haben. Diese Änderungen betrifft nur die Einstellungsdatei, die die Liste der eingetragenen **IKARUS security.manager-Server** enthält.

© 2013 IKARUS Security Software GmbH

6.2.17 Infodialog

6.2.17.1 *Fensteraufbau*

Die Informationen im Dialogfeld **About** ("Über dieses Programm") sind in zwei Bereiche gegliedert:

- **Versionsinformationen:** Zeigt die Versionen der **IKARUS security.manager-Benutzeroberfläche**, des **IKARUS security.manager-Servers** sowie des Updaters an.
- **License Information:** Hier werden das Ablaufdatum und die genutzte bzw. freie Kapazität Ihrer Lizenz angezeigt.

Benutzer können ihre Lizenzen durch Anklicken von **Lizenz erneuern** verlängern (siehe Abbildung 6-65).

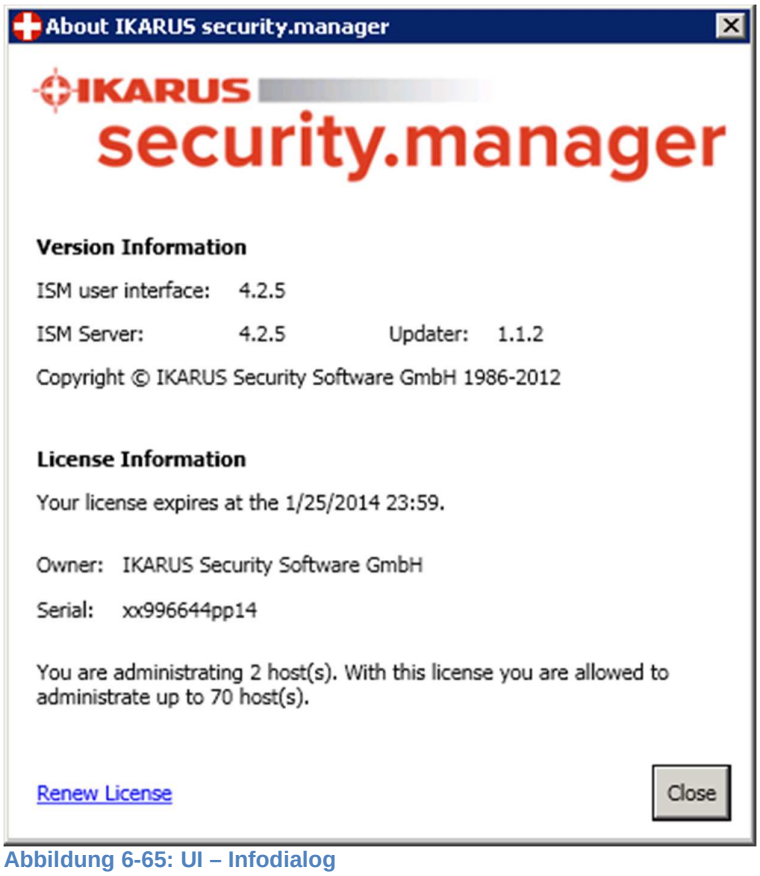

About IKARUS security.manager
IKARUS
security.manager
Version Information
ISM user interface: 4.2.5
ISM Server: 4.2.5 Updater: 1.1.2
Copyright © IKARUS Security Software GmbH 1986-2012
License Information
Your license expires at the 1/25/2014 23:59.
Owner: IKARUS Security Software GmbH
Serial: xx996644pp14
You are administrating 2 host(s). With this license you are allowed to administrate up to 70 host(s).
Renew License
Close

Abbildung 6-65: UI – Infodialog

6.2.18 Die Menüleiste

Die Menüleiste (Abbildung 5-27) befindet sich oben im Hauptfenster der **IKARUS security.manager-UI**.

Sie bietet Zugriff auf die folgenden Untermenüs:

- Datei (Abbildung 5-27)
- Ansicht (Abbildung 5-28)
- Werkzeuge (Abbildung 5-29)
- Hilfe (Abbildung 5-30)

6.2.18.1 *Das Menü „Datei“*

Das Menü **Datei** enthält folgende Optionen:

- **Update ISM (F6):**. Startet den Updatevorgang des ISM-Servers.
- **Beenden (Alt+F4):** Beendet die aktuelle Sitzung und die ISM-UI.
- **Abmelden (Ctrl+Alt+F4):** Beendet die aktuelle Sitzung und das Fenster **Anmeldung**.

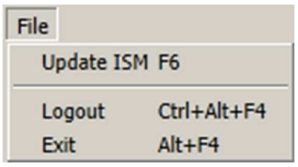


Abbildung 6-66 UI – Menüleiste - Menü "Datei"

6.2.18.2 *Das Menü „Ansicht“*

Das Menü **Ansicht** enthält folgende Optionen:

- **Startseite:** Zeigt oder verbirgt die Übersichtsseite, siehe Abschnitt 6.2.6.
- **Verzeichnis:** Zeigt oder verbirgt das Verzeichnis, siehe Abschnitt 6.2.1.
- **Allgemein:** Zeigt oder verbirgt die Seite Allgemein, siehe Abschnitt 6.2.8/6.2.9.
- **Eigenschaften:** Zeigt oder verbirgt die Eigenschaftsseite, siehe Abschnitt 6.2.7.
- **Anstehende Aufgaben:** Zeigt oder verbirgt das Fenster mit den anstehenden Aufgaben, siehe Abschnitt 6.2.2.
- **Virenliste:** Zeigt oder verbirgt die Virenliste, siehe Abschnitt 6.2.3.
- **Logdatei:** Zeigt oder verbirgt die Logdatei, siehe Abschnitt 6.2.4.
- **Change Log:** Zeigt oder verbirgt das Change Log, siehe Abschnitt 6.2.5.
- **Standardfensteraufbau wiederherstellen:** Stellt den Standardfensteraufbau wieder her.
- **Symbolleiste/Hauptsymbolleiste:** Zeigt oder verbirgt die Hauptsymbolleiste, siehe Abschnitt 6.2.19.
- **IKARUS anti.virus-Konfigurationen:** Öffnet das Konfigurationsfenster von **IKARUS anti.virus**, siehe Abschnitt 6.2.13.

© 2013 IKARUS Security Software GmbH

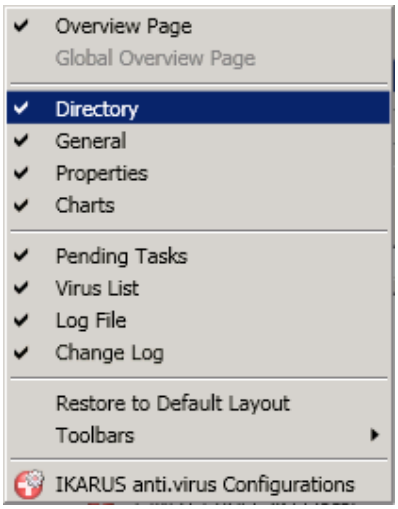


Abbildung 6-67 UI –Menüleiste - Menü "Ansicht"

6.2.18.3 *Das Menü „Werkzeuge“*

Das Menü **Werkzeuge** enthält folgende Optionen:

- **Optionen (F12):** Öffnet das Fenster mit den Optionen für den **IKARUS security.manager**, siehe Abschnitt 6.2.14.
- **Host-Eintragungen aus der Datenbank entfernen:** Mithilfe des Dialogfensters **Host-Eintragungen aus der Datenbank entfernen** lassen sich ungenutzte Hosts aus der Datenbank entfernen. Weitere Informationen zu diesem Dialogfenster finden Sie in Abschnitt 6.2.15.
- **Passwort ändern:** Öffnet ein Fenster, in dem Sie ein neues Passwort für den **IKARUS security.manager** festlegen können.
- **Sprache ändern:** Öffnet ein Fenster, in dem Sie eine andere Sprache für die Benutzeroberfläche des **IKARUS security.manager** festlegen können. Das Programm muss für eine solche Umstellung nicht neu gestartet werden.
- **IKARUS-Virenlexikon:** Öffnet den Standardbrowser und ruft darin das IKARUS-Virenlexikon auf.
- **Support-Informationen speichern:** Erzeugt eine *ZIP*-Datei auf dem **IKARUS security.manager-Server**, die sich auf Ihrem lokalen System ablegen lässt. Weiters wird eine Datenbank-Backup-Datei automatisch erstellt und in das ZIP inkludiert. Damit diese Datei ebenfalls inkludiert werden kann, ist es wichtig, dass der Datenbank-Benutzer Schreibrechte auf dem verteilten Verzeichnis hat und der Rechner, auf dem die Datenbank liegt, muss das verteilte Verzeichnis erreichen können. Diese Datei enthält alle notwendigen Informationen, welche die Support-Abteilung der **IKARUS Security Software** zum Aufrufen von Informationen zu Ihrem System benötigt.

© 2013 IKARUS Security Software GmbH

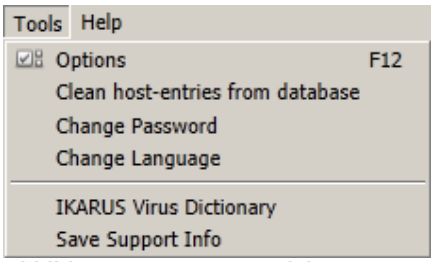


Abbildung 6-68: UI – Menüleiste, Menü „Werkzeuge“

6.2.18.4 *Das Menü „Hilfe“*

Das Menü **Hilfe** enthält folgende Optionen:

- **Benutzerhandbuch (F1):** Öffnet das vorliegende Benutzerhandbuch für den **IKARUS security.manager**.
- **Kontaktinformationen:** Öffnet das Fenster **Kontaktinformationen**.
- **Allgemeine Geschäftsbedingungen:** Öffnet die Allgemeinen Geschäftsbedingungen für den **IKARUS security.manager**.
- **Über den IKARUS security.manager:** Öffnet ein Fenster mit Informationen zur verwendeten Version des **IKARUS security.manager** und zur benutzten Lizenz.

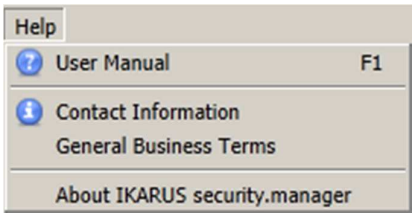


Abbildung 6-69: UI – Menüleiste, Menü „Hilfe“

6.2.18.5 *Das Menü „Management“*

Das Menü **Management** ist nur im **Management-Modus aktiv** und enthält folgende Menüpunkte:

- **Optionen:** Öffnet das Fenster Optionen für den Management-Modus (siehe Kapitel 6.2.16.1)
- **Konfigurationsdatei exportieren:** Ermöglicht das Exportieren bereits eingetragener **IKARUS security.manager-Server** (siehe Kapitel 6.2.16.2).
- **Ändern Sie das Passwort für den Management-Modus:** Mit Hilfe dieses Menüpunkts können Sie das Passwort für die Anmeldung verändern (siehe Kapitel 6.2.16.3). Zu beachten gilt jedoch, dass diese Passwortänderung keine Auswirkungen auf die Passwörter der eingetragenen **IKARUS security.manager-Server** haben.

© 2013 IKARUS Security Software GmbH

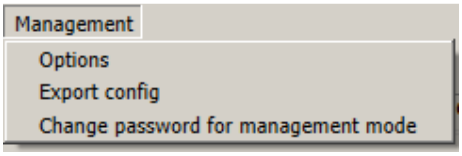


Abbildung 6-70: UI – Menüleiste, Menü „Management“

© 2013 IKARUS Security Software GmbH

6.2.19 Die Symbolleiste

Die **Symbolleiste** (Abbildung 6-71) befindet sich oben im Hauptfenster der Benutzeroberfläche des **IKARUS security.manager** direkt unter der *Menüleiste*. Ein Klick auf **IKARUS anti.virus - Konfigurationen** öffnet das **IKARUS security.manager**-Konfigurationsfenster. Weitere Informationen dazu finden Sie in Abschnitt 6.2.13.

6.2.19.1 *Fensteraufbau*

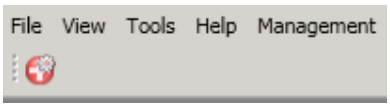


Abbildung 6-71: UI – Symbolleiste

© 2013 IKARUS Security Software GmbH

7 Geteiltes Verzeichnis

Das „geteilte Verzeichnis“ ist die *Netzwerkfreigabe*, auf der die ausführbare Datei *ismxstartup.exe* abgelegt wird. Da diese ausführbare Datei für die Installation der **IKARUS anti.virus** auf einem *Client* benötigt wird, muss der betreffende *Client* über Lesezugriff auf die Freigabe und die Datei verfügen. Des Weiteren benötigt der **IKARUS security.manager-Server** Schreibzugriff auf die *Netzwerkfreigabe*, um die Datei dort überhaupt ablegen zu können. Sie können das geteilte Verzeichnis auf der Registerkarte ***Allgemein*** (Abbildung 5-22) der des Fensters ***IKARUS security.manager-Einstellungen*** angeben.

Bitte überprüfen Sie, ob der Rechner auf dem die Datenbank läuft, auf das verteile Verzeichnis zugreifen kann. Außerdem benötigt der Datenbank-Benutzer ebenfalls Schreibrechte, da es sonst nicht möglich ist, während der Generierung des Support.zip die Datenbank-Backup-Datei zu erstellen. Die Datenbank-Backup-Datei wird auf dem geteilten Verzeichnis zwischengespeichert und nach der Verarbeitung wieder gelöscht.

© 2013 IKARUS Security Software GmbH

8 Lizenzinformationen

Damit Sie Ihr Netzwerk schützen und den **IKARUS security.manager** einsetzen können, benötigen Sie eine gültige Lizenz. Eine Lizenz umfasst eine definierte Anzahl von Benutzerlizenzen, die entsprechend der Größe Ihres Unternehmens auszuwählen ist. Die **IKARUS security.manager**-Lizenz wird von allen *Clients*, die zur Verwaltung ausgewählt sind, gemeinsam verwendet. Es ist nicht möglich, mehr **IKARUS anti.virus**-Instanzen im Netzwerk zu betreiben und zu verwalten, als in der Lizenz definiert sind. Für nicht verwaltete *Clients* liegt unter Umständen bereits eine gültige Lizenz vor, sofern Sie sie bereits zu einem früheren Zeitpunkt angeschafft haben. Sollte dies jedoch nicht der Fall sein und können Sie keine weiteren *Clients* zur Verwaltung hinzufügen, weil Sie das *Client*limit Ihrer aktuellen **IKARUS security.manager**-Lizenz bereits erreicht haben, dann sind diese überzähligen Clients nicht durch **IKARUS anti.virus** geschützt und deswegen nicht sicher. **Clients, für die keine gültige Lizenz vorliegt, stellen deswegen eine potenzielle Gefahr für Ihr gesamtes Netzwerk dar!**

8.1 Registrierung

Wenn für den **IKARUS security.manager** keine gültige Lizenz vorliegt, öffnet sich das in Abbildung 8-1: UI – IKARUS security.manager-Registrierung gezeigte Dialogfeld, und Sie werden aufgefordert, eine gültige Lizenz in Form einer IKARUS-Lizenzdatei oder eines *IKARUS-Aktivierungsschlüssels* abzugeben.

Im Dialogfeld **Registrierung** kann eine der beiden folgenden Möglichkeiten zum Registrieren Ihres **IKARUS security.manager** ausgewählt werden:

- **Lizenzdatei:** Öffnet einen Dateibrowser, in dem Sie die gewünschte IKARUS-Lizenzdatei auswählen können.
- **Aktivierungsschlüssel:** Öffnet das Aktivierungsfenster, siehe Abschnitt 8.2.

8.1.1 Fensteraufbau

IKARUS security.manager Registration
No valid License available!
Please renew your License by clicking on 'License File'.
If you have an Activation Code, please click on 'Activation Key' and fill out the form correctly.
For any further questions contact us via support@ikarus.at or under +43 / 01 / 589 95 - 0.
License File
Activation Key

Abbildung 8-1: UI – IKARUS security.manager-Registrierung

8.2 Aktivierungsschlüssel

© 2013 IKARUS Security Software GmbH

Wenn Sie statt einer IKARUS-Lizenzdatei einen *IKARUS-Aktivierungsschlüssel* erhalten haben, können Sie eine gültige Lizenz über das Dialogfeld Lizenzaktivierung (Abbildung 8-2) abrufen. Geben Sie einfach die angeforderten Informationen ein, und verschicken Sie die Daten. Sie erhalten nach erfolgreicher Übermittlung der Daten eine E-Mail mit einer Lizenzdatei in der Anlage an die von Ihnen angegebene E-Mail-Adresse. Alle mit einem Sternchen gekennzeichneten Felder sind unbedingt auszufüllen.

8.2.1 Fensteraufbau

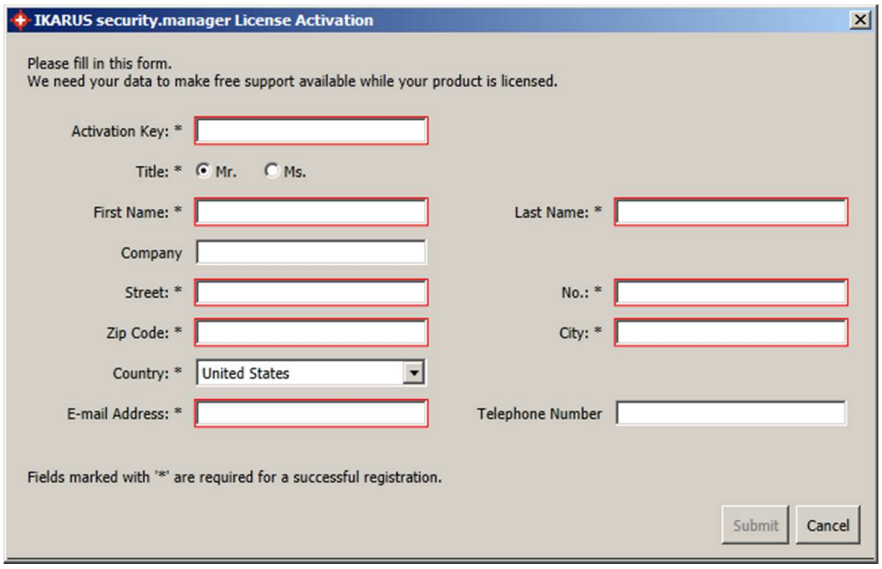


Abbildung 8-2: UI – IKARUS security.manager-Lizenzaktivierung

© 2013 IKARUS Security Software GmbH

9 Softwareverteilung

Die Installations- und Deinstallationsprozesse für die **IKARUS anti.virus** sind in verschiedene Schritte unterteilt. Für eine erfolgreiche und vollständige Ausführung des jeweiligen Prozesses müssen die folgenden Bedingungen erfüllt sein:

- Für den **IKARUS security.manager-Server** muss ein *geteiltes Verzeichnis* (Abbildung 5-22) vorhanden sein, in dem die für die Remoteinstallation erforderlichen Binärdateien abgelegt werden können.
- Der **IKARUS security.manager-Server** muss über die erforderlichen Rechte verfügen, um Binärdateien remote auf dem Ziel*client* auszuführen. Wurde der **IKARUS security.manager-Server** mit einem *Domänen*administratorkonto installiert und befindet sich der Ziel*client* in derselben *Domäne* wie der **IKARUS security.manager-Server**, dann sind für diesen *Client* keine weiteren Einstellungen erforderlich. Andernfalls müssen Sie Anmeldeinformationen angeben, die über die zur Ausführung der Aufgaben erforderlichen Rechte auf dem Ziel*client* verfügen. Dies können Sie im Bereich „*Rechteverwaltung*“ eines *Clients* aus der **IKARUS security.manager-UI** heraus tun.
- Der Ziel*client* benötigt zumindest Lesezugriff auf das benutzerseitig festgelegte geteilte Verzeichnis, da er von dort die Binärdatei *ismxstartup* abrufen können muss.
- Falls Sie eine Firewall verwenden, muss die Weiterleitung der Kommunikation über die betreffenden *TCP*-Ports aktiviert werden.
- Der Ziel*client* muss die Hardware- und Softwareanforderungen für den Betrieb der **IKARUS anti.virus** erfüllen.
- Die Option ***Clientupdate erzwingen*** muss im Fenster ***IKARUS security.manager-Einstellungen*** (Abbildung 5-22) aktiviert sein.

© 2013 IKARUS Security Software GmbH

9.1 *IKARUS anti.virus* installieren

Zur Installation und Bereitstellung der **IKARUS anti.virus** klicken Sie mit der rechten Maustaste auf einen *Client* oder eine Gruppe im *Verzeichnis*. Im nun erscheinenden Kontextmenü klicken Sie auf den Eintrag anti.***virus installieren*** (Abbildung 5-8). Die Installation der **IKARUS anti.virus** umfasst die nachfolgend aufgeführten Schritte (vgl. Abbildung 8-1). Da die Installation eine gewisse Zeit in Anspruch nehmen kann, bitten wir um Ihre Geduld.

- Schritt 1: Der **IKARUS security.manager-Server** speichert die erforderlichen ausführbaren Dateien im *geteilten Verzeichnis*.
- Schritt 2: Der **IKARUS security.manager-Server** versucht nun, den *Dienst ismxstartup* aus dem *geteilten Verzeichnis* heraus remote zu installieren. Der Ziel*client* benötigt zumindest Lesezugriff auf das *geteilte Verzeichnis* und die darin enthaltenen Dateien.
- Schritt 3: Der *Dienst ismxstartup* ruft die Binärdatei *guardxup* vom **IKARUS security.manager-Server** ab, speichert sie im Windows-Temporärverzeichnis des Ziel*clients* und führt sie dort aus.
- Schritt 4: Die Binärdatei *guardxup* führt nun alle weiteren für die Installation der **IKARUS anti.virus** auf dem Zielclient erforderlichen Schritte aus. Dies umfasst das Abrufen der **IKARUS anti.virus**-Binärdateien vom **IKARUS security.manager-Server** und ihre Installation auf dem Zielhost.

© 2013 IKARUS Security Software GmbH

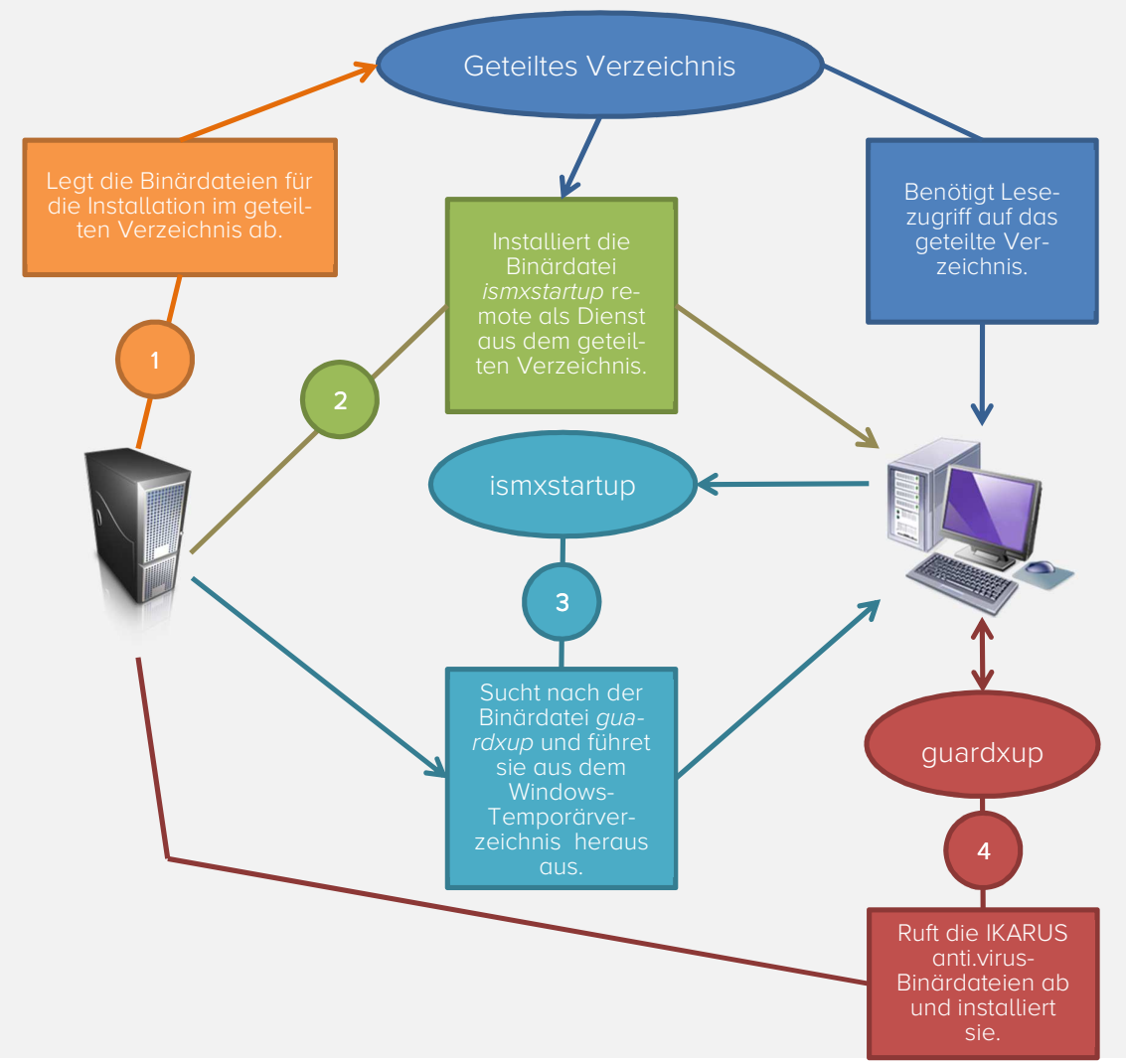

Geteiltes Verzeichnis
Legt die Binärdateien für die Installation im geteilten Verzeichnis ab.
Installiert die Binärdatei *ismxstartup* remote als Dienst aus dem geteilten Verzeichnis.
Benötigt Lesezugriff auf das geteilte Verzeichnis.
1
2
ismxstartup
3
Sucht nach der Binärdatei *guardxup* und führet sie aus dem Windows-Temporärverzeichnis heraus aus.
guardxup
4
Ruft die IKARUS anti.virus-Binärdateien ab und installiert sie.

Abbildung 9-1: Softwareverteilung – Installationsprozess

© 2013 IKARUS Security Software GmbH

9.2 *IKARUS anti.virus* deinstallieren

Zur Deinstallation der **IKARUS anti.virus** klicken Sie mit der rechten Maustaste auf einen *Client* oder eine Gruppe im Verzeichnis. Im nun erscheinenden Kontextmenü klicken Sie auf den Eintrag anti.***virus deinstallieren*** (vgl. Abbildung 5-8). Hinweis: Die Deinstallation ist nur auf *verwalteten Clients* möglich.

© 2013 IKARUS Security Software GmbH

10 Konfigurationsdatei

Die Konfigurationsdatei namens *ism.conf* ist im Verzeichnis *conf* des Installationsziels vorhanden, das Sie bei der Installation des **IKARUS security.manager-Servers** angegeben haben (siehe Abschnitt 5.1.11). Hier können die Angaben für die Verbindung zur *MSSQL*-Datenbank gemacht sowie die *LDAP*-Verbindungseinstellungen und die *TCP*-Ports festgelegt werden, die für die Kommunikation zwischen den **IKARUS anti.virus** und dem **IKARUS security.manager** verwendet werden.

Beispiel einer Konfigurationsdatei:

```
<config>
    dbconnstring        DRIVER={SQL Server};SERVER=localhost
    serverport          9887
    clientupdateport    9888
</config>

<ldap>
    type                native
    servername          esx-2k8-de-srv.labor.local
    searchpath          dc=labor,dc=local
    authmethod          simple
    username            LDAP Connector
    password            none
    attribute           dNSHostName
    filter              (objectCategory=computer)
</ldap>
```

Anmerkung: Die *LDAP*-Parameter lassen sich über die **IKARUS security.manager**-Einstellungen innerhalb der Benutzeroberfläche des **IKARUS security.manager** bearbeiten. Mehr Informationen dazu finden Sie in Abschnitt 6.2.14.6

© 2013 IKARUS Security Software GmbH

10.1 Der Abschnitt <config>

Im Abschnitt <*config*> können Sie Informationen zur *MSSQL*-Datenbank, die vom **IKARUS security.manager-Server** für die Speicherung von Daten und Einstellungen verwendet wird, sowie zu den für die Kommunikation verwendeten *TCP*-Ports angeben.

Einstellung	Beschreibung
dbconnstring	Information zur Herstellung einer Verbindung mit der *MSSQL*-Zieldatenbank. Sie können hier den Namen des Servers, auf dem die Datenbank installiert ist, und Authentifizierungsmethoden angeben, die für den Zugriff auf die Datenbank erforderlich sind. Weitere Informationen zur Syntax und zu vorhandenen Eigenschaften des Connection-Strings entnehmen Sie Ihrer *MSSQL*-Dokumentation.
serverport	Hier wird der *TCP*-Port angegeben, der für die Kommunikation zwischen **IKARUS security.manager-Server** und **IKARUS security.manager-UI** verwendet werden soll. Stellen Sie sicher, dass dieser Port weitergeleitet wird, falls Sie eine *Firewall* verwenden.
clientupdateport	Dieser *TCP*-Port wird für die Kommunikation zwischen den Updatebinärdateien und den **IKARUS anti.virus** benutzt. Stellen Sie sicher, dass dieser Port weitergeleitet wird, falls Sie eine *Firewall* verwenden.
timespanAD	Erlaubt Werte zwischen **1 und 24**, was bedeutet, dass ab Eingabe des betreffenden Werts X (bzw. ab Neustart des Servers) alle X Stunden das *Aktive Verzeichnis* neu geladen wird. Die Standardeinstellung des *AV* ist intern auf **"alle 12 Stunden"** eingestellt. Bei Festlegung dieser Einstellung in der config-Datei
dailytimeAD	Erlaubt Werte zwischen **0 und 23**, was bedeutet, dass das *AV* täglich zur jeweils festgelegten Uhrzeit neu geladen wird. Diese Einstellungsoption lässt sich nicht in Verbindung mit der **timespanAD**-Einstellung verwenden, da diese die **dailytimeAD**-Einstellung stets aufhebt.

© 2013 IKARUS Security Software GmbH

10.2 Der Abschnitt <ldap>

Im Abschnitt <*ldap*> geben Sie Informationen zu dem *LDAP*-*Server* an, mit dem der **IKARUS security.manager-Server** zur Auflösung von Clients, die sich in Ihrem *Active Directory* befinden, eine Verbindung herstellen muss. Ist kein <*ldap*>-Abschnitt in Ihrer *Konfigurationsdatei* vorhanden, dann versucht der **IKARUS security.manager-Server**, die entsprechenden Informationen direkt beim *Domänen-controller* abzurufen.

Einstellung	Beschreibung
type	Typ der *LDAP*-Konfiguration
servername	Name des *Domänencontrollers*
searchpath	Definiert die zu scannende Domäne. Verschiedene *Domänen*ebenen werden durch das Schlüsselwort *dc* (*Domänen*komponente) voneinander getrennt. Beispiel für eine Domäne namens *.company.local*: searchpath dc=company dc=local
authmethod	Gibt an, welche Methode zur Authentifizierung am *Domänencontroller* verwendet werden soll. Wenn Sie keinen bestimmten Benutzer authentifizieren möchten, können Sie hier den Wert *anonymous* definieren.
username	Hiermit wird der Benutzername festgelegt, mit dem die Authentifizierung am *Domänencontroller* erfolgen soll. Dieser wird nur benötigt, wenn als Authentifizierungsmethode nicht *anonymous* ausgewählt wurde.
password	Hiermit wird das Passwort festgelegt, mit dem die Authentifizierung am *Domänencontroller* erfolgen soll. Dieses wird nur benötigt, wenn als Authentifizierungsmethode nicht *anonymous* ausgewählt wurde.
attribute	Bestimmt das Attribut, das ausgelesen werden soll.
filter	Legt das Kriterium fest, anhand dessen der für *attribute* definierte Wert aufgelöst wird.

© 2013 IKARUS Security Software GmbH

11 Abbildungsverzeichnis

Abbildung 5-1: Serverinstallation – Willkommen ..... - 13 -
Abbildung 5-2: Serverinstallation – Lizenzvertrag ..... - 14 -
Abbildung 5-3: Serverinstallation – LDAP-Einstellungen ..... - 19 -
Abbildung 5-4: Serverinstallation – Bereitstellungseinstellungen ..... - 20 -
Abbildung 5-5: Serverinstallation – BenutzereinstellungenError! Bookmark not defined.
Abbildung 5-6: Serverinstallation – NetzwerkeinstellungenError! Bookmark not defined.
Abbildung 5-7: Serverinstallation – Installation von SQL ExpressError! Bookmark not defined.
Abbildung 5-8 Server-Installation – DatenbankeinstellungenError! Bookmark not defined.
Abbildung 5-9: Serverinstallation – Installationsordner auswählen ..... - 21 -
Abbildung 5-10: Serverinstallation – Installation bestätigen ..... - 22 -
Abbildung 5-11: Serverinstallation – Installation abgeschlossen ..... - 25 -
Abbildung 5-12: UI-Installation – Willkommen ..... - 28 -
Abbildung 5-13: UI-Installation – Lizenzvertrag ..... - 29 -
Abbildung 5-14: UI-Installation – Installationsordner auswählen ..... - 31 -
Abbildung 5-15: UI-Installation – Installation bestätigen ..... - 32 -
Abbildung 5-16: UI-Installation – Installation abgeschlossen ..... - 33 -
Abbildung 6-1: UI – Anmeldung (Einzel-Modus) ..... - 35 -
Abbildung 6-2: UI – Anmeldung (Management-Modus) ..... - 36 -
Abbildung 6-3: UI –Passwort festlegen (Einzel-Modus) ..... - 37 -
Abbildung 6-4: UI –Passwort festlegen (Management-Modus) ..... - 38 -
Abbildung 6-5: UI – Change Management ..... - 40 -
Abbildung 6-6: UI – Lizenzverletzung ..... - 42 -
Abbildung 6-7: UI – Benutzeroberfläche ..... - 44 -
Abbildung 6-8: UI – Verzeichnis (Einzel-Modus) ..... - 45 -
Abbildung 6-9 UI - Verzeichnissymbolleiste ..... - 46 -
Abbildung 6-10 Die Scanoptionen ..... - 46 -
Abbildung 6-11 Das Kontextmenü für clientbezogene Aktionen ..... - 47 -
Abbildung 6-12 Optionen für die Verwaltung bzw. das Ausnehmen von der Verwaltung ..... - 47 -
Abbildung 6-13 Die Gruppen/Clientstruktur ..... - 48 -
Abbildung 6-14 Das Kontextmenü für eine Gruppe bzw. einen Client ..... - 48 -
Abbildung 6-15 UI – Verzeichnisfilter ..... - 49 -
Abbildung 6-16: UI – Anstehende Aufgaben ..... - 52 -
Abbildung 6-17: UI – Aufgabendetails ..... - 54 -
Abbildung 6-18: UI – Virenliste ..... - 56 -
Abbildung 6-19: UI – Virusinformationen ..... - 57 -
Abbildung 6-20: UI – Logdatei ..... - 58 -
Abbildung 6-21: UI – Change Log ..... - 59 -
Abbildung 6-22: UI – Startseite ..... - 61 -
Abbildung 6-23: UI – Eigenschaftsseite ..... - 64 -
Abbildung 6-24: UI – Seite „Allgemein“ für Gruppen ..... - 66 -
Abbildung 6-25: UI – Seite „Allgemein“ für Clients ..... - 67 -
Abbildung 6-26: UI – Benachrichtigungsleiste ..... - 68 -
Abbildung 6-27 UI –Diagrammseite ..... - 70 -
Abbildung 6-28 UI – Globale Startseite ..... - 71 -

© 2013 IKARUS Security Software GmbH

Abbildung 6-29 UI – Globale Startseite - Kontextmenü ..... - 72 -
Abbildung 6-30: UI – IKARUS anti.virus-Konfigurationen ..... - 73 -
Abbildung 6-31: „IKARUS anti.virus-Konfiguration“, Registerkarte „Allgemein“ ..... - 74 -
Abbildung 6-32: „IKARUS anit.virus-Konfiguration“, Registerkarte „E-Mail“ ..... - 75 -
Abbildung 6-33: „IKARUS anti.virus-Konfiguration“, Registerkarte „Update“ ..... - 76 -
Abbildung 6-34: „IKARUS anti.virus -Konfiguration“, Registerkarte „Dial-Up-Verbindungen“ ..... - 77 -
Abbildung 6-35: „IKARUS anti.virus-Konfiguration“, Registerkarte „Ausnahmen“ (Prozessausnahme) ..... - 78 -
Abbildung 6-36: „IKARUS anti.virus-Konfiguration“, Registerkarte „Logs“ ..... - 79 -
Abbildung 6-37: „IKARUS anti.virus-Konfiguration“, Registerkarte „Extras“ ..... - 80 -
Abbildung 6-38: „IKARUS anti.virus-Konfiguration“, Registerkarte „Anti-Spam“ ..... - 81 -
Abbildung 6-39: Dialogfeld „Konfiguration erweiterter Spamschutz“ ..... - 82 -
Abbildung 6-40: „IKARUS anti.virus-Konfiguration“, Registerkarte „Scans“ ..... - 83 -
Abbildung 6-41: „IKARUS anti.virus-Konfiguration“, Dialogfeld „Scan-Profil hinzufügen“ ..... - 83 -
Abbildung 6-42: „IKARUS security.manager-Einstellungen“, Registerkarte „Allgemein“ ..... - 86 -
Abbildung 6-43: „IKARUS security.manager-Einstellungen“, Registerkarte „E-Mail-Benachrichtigungen“ ..... - 87 -
Abbildung 6-44: „IKARUS security.manager-Einstellungen“, Registerkarte „Berichte“ .- 88 -
Abbildung 6-45: „IKARUS security.manager-Einstellungen“, Registerkarte „Update“ ...- 89 -
Abbildung 6-46 UI –Einstellungen IKARUS security.manager, "Fileshare" ..... - 90 -
Abbildung 6-47 UI – Einstellungen IKARUS security.manager – LDAP ..... - 92 -
Abbildung 6-48 Diagrammoptionen ..... - 93 -
Abbildung 6-49 Einstellungen PDF-Bericht ..... - 94 -
Abbildung 6-50 UI – Host-Einträge aus der Datenbank entfernen ..... - 95 -
Abbildung 6-51 : UI - Menü "Management", Menüpunkt "Konfigurationsdatei exportieren" ..... - 97 -
Abbildung 6-52 : UI – Optionen Dialog ..... - 98 -
Abbildung 6-53 : UI – Kontextmenü im Optionen Dialog ..... - 98 -
Abbildung 6-54 : UI – Bearbeiten Dialog ..... - 99 -
Abbildung 6-55 : UI – Bearbeiten Dialog, Eingabe ungültiger Daten ..... - 100 -
Abbildung 6-56 : UI – Bearbeiten Dialog, Passwort für eine neue Installation ändern ..- 100 -
Abbildung 6-57 : UI – Bearbeiten Dialog, Überprüfung der Zugangsdaten ..... - 101 -
Abbildung 6-58: UI - Menü "Management", Menüpunkt "Konfigurationsdatei exportieren" ..... - 102 -
Abbildung 6-59: UI Dialog "Konfigurationsdatei exportieren“ – Auswahl der zu exportierenden ISM Instanzen ..... - 103 -
Abbildung 6-60: UI - Dialog "Konfigurationsdatei exportieren“ – Fehlermeldung bei ungültigem Passwort ..... - 104 -
Abbildung 6-61: UI - Dialog "Konfigurationsdatei exportieren“ – Gültiges Passwort .....- 105 -
Abbildung 6-62: UI – Datei-Speichern Dialog für den Export der Konfigurationsdatei ..- 105 -
Abbildung 6-63: UI – Ändern Sie das Passwort fur den Management-Modus ..... - 106 -
Abbildung 6-64: UI – Infodialog ..... - 107 -
Abbildung 6-65 UI – Menüleiste - Menü "Datei" ..... - 108 -

© 2013 IKARUS Security Software GmbH

Abbildung 6-66 UI –Menüleiste - Menü "Ansicht" - 109 -
Abbildung 6-67: UI – Menüleiste, Menü „Werkzeuge“ - 110 -
Abbildung 6-68: UI – Menüleiste, Menü „Hilfe“ - 110 -
Abbildung 6-69: UI – Menüleiste, Menü „Management“ - 111 -
Abbildung 6-70: UI – Symbolleiste - 112 -
Abbildung 8-1: UI – IKARUS security.manager-Registrierung - 114 -
Abbildung 8-2: UI – IKARUS security.manager-Lizenzaktivierung - 115 -
Abbildung 9-1: Softwareverteilung – Installationsprozess - 118 -

© 2013 IKARUS Security Software GmbH

12 Glossar

Abkürzung	Benennung	Beschreibung
	IKARUS Anti.Virus	DIe IKARUS virus.utilities werden 2012 auf IKARUS anti.virus umbenannt, weswegen sie in diesem Dokument bereits die neue Benennung finden.
	Windows-Dienst	Ein Windows-Dienst ist eine Datei, deren Ausführung im Hintergrund vorgesehen ist, ohne dass der Benutzer hierzu tätig werden müsste. Windows-Dienste können so konfiguriert sein, dass sie nach Abschluss der Windows-Startsequenz automatisch gestartet werden. Windows-Dienste können wahlweise mit lokalen Systemkonten oder einem Benutzerkonto in Ihrem Windows-Netzwerk als Anmeldekonto installiert werden.
MSSQL	Microsoft Structured Query Language	Der Microsoft SQL-Server ist ein relationaler Datenbankserver, der von Microsoft entwickelt wurde. Es handelt sich um ein Softwareprodukt, dessen primäre Funktion im von anderen Softwareanwendungen angeforderten Speichern und Abrufen von Daten besteht. Diese Softwareanwendungen können sowohl auf demselben Computer als auch auf einem anderen Computer ausgeführt und über ein Netzwerk (einschließlich des Internets) angebunden sein.
TCP	Transmission Control Protocol	Das TCP-Protokoll ist eines der wichtigsten Protokolle der Internetprotokollfamilie. Es handelt sich bei TCP um eine der beiden Ursprungskomponenten dieser Protokollfamilie, die das *Internet Protocol* (IP) ergänzt, weswegen die gesamte Protokollfamilie häufig als „TCP/IP“ bezeichnet wird. TCP ermöglicht die zuverlässige und geordnete Zustellung eines Bytestroms von einem Programm auf einem Computer an einen anderen Computer.
IP	Internet Protocol	Das Internet Protocol ist das wichtigste Kommunikationsprotokoll bei der Weiterleitung von *Datagrammen* (Paketen) innerhalb eines *Netzwerkverbunds* unter Verwendung der Internetprotokollfamilie. Als Protokoll, das für die Weiterleitung von Paketen über Netzwerkgrenzen hinweg zuständig ist, bildet es die

© 2013 IKARUS Security Software GmbH

		Grundlage für das *Internet*.
LDAP	Lightweight Directory Access Protocol	LDAP ist ein Anwendungsprotokoll für den Zugriff auf verteilte Verzeichnisinformations-dienste und die Pflege solcher Dienste über ein *IP*-Netzwerk.
	Proxy-Server	In Computernetzen bezeichnet dieser Begriff einen Server (d. h. ein Computersystem oder eine *Anwendung*), der als Zwischenglied für Anfragen von *Clients* dient, die Ressourcen von anderen *Servern* anfordern.
	Netzwerkfreigabe	In der Computertechnik ist eine freigegebene Ressource oder Netzwerkfreigabe ein Gerät oder ein Datenbestand auf einem Computer, auf dem von einem anderen Computer aus remote zugegriffen werden kann. Der Zugriff erfolgt in der Regel über ein *LAN* oder das *Intranet* eines Unternehmens in transparenter Form, d. h., so als ob sich die Ressource auf dem lokalen Computer befände.
LAN	Local Area Network	Ein LAN ist ein Computernetzwerk, das Com-puter in einem eingeschränkten geographi-schen Bereich – einem Haus, einer Schule, einem Rechenzentrum oder einem Büroge-bäude – miteinander verbindet.
	Intranet	Ein Intranet ist ein Computernetzwerk, das auf der Basis der *IP*-Technologie die sichere ge-meinsame Nutzung beliebiger Informationen oder des Netzwerkbetriebssystems des Un-ternehmens gestattet.
AD	Active Directory	Active Directory ist ein *Verzeichnisdienst*, der von Microsoft für Windows-Domänennetzwerke entwickelt wurde. Es ist Bestandteil der meisten Windows Server-Betriebssysteme. Servercomputer, auf denen Active Directory ausgeführt wird, heißen *Do-mänencontroller*.
	Windows-Domäne	Eine Windows-Domäne ist eine Sammlung von so genannten Sicherheitsprinzipalen, die eine zentrale Verzeichnisdatenbank gemeinsam verwenden. Diese zentrale Datenbank (seit Windows 2000 als „*Active Directory*“ bekannt[1], unter Windows Server 2008 und Windows Server 2008 R2 als „*Active Directory*-Domänendienste“ bezeichnet, des Weiteren unter Windows NT-

© 2013 IKARUS Security Software GmbH

		Betriebssystemen auch „NT-Verzeichnisdienste“, kurz NTDS genannt) enthält die Benutzerkonten und Sicherheitsinformationen für die Ressourcen in der betreffenden Domäne. Jede Person, die Computer innerhalb einer Domäne verwendet, erhält genau ein eindeutiges Konto samt Benutzername. Diesem Konto kann dann der Zugriff auf Ressourcen innerhalb der Domäne gestattet werden.
	Verzeichnisdienst	Als Verzeichnisdienst bezeichnet man das Softwaresystem, in dem Informationen in einem Verzeichnis gespeichert und organisiert werden und das Zugriff auf diese Informationen ermöglicht. In der Softwaretechnik ist ein Verzeichnis eine Zuordnung von Namen und Werten. Es gestattet das Nachschlagen von zu einem Namen gehörenden Werten ähnlich wie ein Lexikon.
DC	Domänencontroller	Auf Windows Server-Systemen ist ein Domänencontroller ein *Server*, der Authentifizierungsanforderungen (Anmeldungen, Berechtigungsprüfungen usw.) in einer *Windows Server-Domäne* bearbeitet. Eine Domäne ist ein mit Windows NT eingeführtes Konzept, das einem Benutzer bei Angabe einer korrekten Kombination aus Benutzername und Passwort den Zugriff auf eine Anzahl von Computerressourcen gestattet.
	Server	Im Kontext der Client/Server-Architektur ist ein Server ein Computerprogramm, dessen Aufgabe bei der Ausführung darin besteht, die Anfragen anderer Programme – der *Clients* – zu bearbeiten. Das bedeutet, dass der Server im Auftrag der *Clients* bestimmte Computeraufgaben erledigt. Die *Clients* werden entweder auf demselben Computer ausgeführt oder sind über das Netzwerk mit dem Server verbunden.
	Client	Ein Client ist eine Anwendung oder ein System, das auf einen Dienst zugreift, der von einem *Server* bereitgestellt wird. Der *Server* wird häufig (aber nicht immer) auf einem anderen Computersystem ausgeführt; in diesem Fall greift der Client über ein Netzwerk auf den Dienst zu.

© 2013 IKARUS Security Software GmbH

FQDN	Fully Qualified Domain Name	Ein vollqualifizierter Domänenname (manchmal auch als „absoluter Domänenname“ bezeichnet) ist ein Domänenname, der seinen exakten Standort in der hierarchischen Baumstruktur des *Domain Name System (DNS)* angibt. Aufgeführt werden alle Domänenebenen einschließlich der *Top-Level-Domain* und der *Stammzone*. Ein vollqualifizierter Domänenname unterscheidet sich stets in seiner Eindeutigkeit: Er kann nur auf genau eine Weise interpretiert werden.
	Domänenname	Ein Domänenname ist eine für Identifizierungszwecke vorgesehene Zeichenfolge, die einen Bereich im Internet bezeichnet, der der autonomen Kontrolle genau einer Einrichtung unterliegt. Domänennamen werden entsprechend den Regeln und Prozeduren des *Domain Name System (DNS)* gebildet.
DNS	Domain Name System	DNS ist ein hierarchisches, verteiltes Benennungssysteme für Computer, Dienste und andere Ressourcen, die mit dem Internet oder mit einem privaten Netzwerk verbunden sind. Es verknüpft verschiedene Informationen mit *Domänennamen*, die allen teilnehmenden Entitäten zugewiesen werden. Der wichtigste Aspekt ist jedoch, dass DNS die Übersetzung von für den Menschen verständlichen *Domänennamen* in numerische Adressen durchführt, die von Netzwerkgeräten verwendet werden, um die entsprechenden Geräte weltweit zu ermitteln und mit ihnen zu kommunizieren.
TLD	Top Level Domain	Eine Top-Level-Domain ist eine Domäne auf der obersten Ebene im *Domain Name System (DNS)* des Internets. Die Namen von Top-Level-Domains sind in der *Stammzone* des Namespace installiert. Bei allen Domänen untergeordneter Ebenen bildet die Top-Level-Domain den letzten Teil des *Domänennamens*, d. h. den letzten Partikel eines *FQDN*.
	Stammzone	Eine Stammzone ist die oberste DNS-Zone in einem hierarchischen Namespace, der das *Domain Name System (DNS)* verwendet. In der Regel bezieht sich die Bezeichnung auf die Stammzone des größten globalen Netz-

© 2013 IKARUS Security Software GmbH

		werks, also des Internets.
	DNS-Zone	Eine DNS-Zone ist ein Teil eines *Domänennamen*sraums, der auf dem *Domain Name System (DNS)* basiert und dessen administrative Zuständigkeit delegiert wurde.
	IKARUS-Aktivierungsschlüssel	
	Verwalten	In der Terminologie des **IKARUS security.manager** versteht man unter „Verwaltung“ (oder „Administration“), dass ein *Client*, auf dem die **IKARUS anti.virus** installiert sind, durch den **IKARUS security.manager** verwaltet wird, d. h., der Client bezieht Updates, Konfigurationen, Lizenzen und Einstellungen vom **IKARUS security.manager**. Bei nicht verwalteten *Clients* wird lediglich eine Statusinformation angezeigt. Wie viele *Clients* Sie verwalten können, ist in der verwendeten Lizenz definiert.
	Anwendung (Software)	Eine Anwendungssoftware (auch als „Anwendung“, „Applikation“ oder kurz „App“ bezeichnet) ist eine *Computersoftware*, die dem Benutzer bei der Durchführung bestimmter Aufgaben helfen soll.
	Computersoftware	Computersoftware (auch kurz als „Software“ bezeichnet) ist eine Sammlung von Computerprogrammen und zugehörigen Daten, denen ein Computer Anweisungen dazu entnimmt, was er wie zu tun hat. Anders gesagt ist Software eine konzeptionelle Entität, also eine Gruppe von Computerprogrammen, Prozeduren und der zugehörigen Dokumentation, die mit dem Betrieb eines Datenverarbeitungssystems in Zusammenhang stehen.
	Firewall	Eine Firewall ist ein Gerät oder ein Geräteverbund, dessen Aufgabe darin besteht, Datenübertragungen aus einem und in ein Netzwerk auf der Basis von Regeln zuzulassen bzw. zu blockieren. Firewalls werden häufig eingesetzt, um Netzwerke vor dem Zugriff durch Unbefugte zu schützen, gleichzeitig jedoch rechtmäßige Kommunikationsvorgänge zuzulassen.

© 2013 IKARUS Security Software GmbH

	ZIP	Bei ZIP handelt es sich um ein **Dateiformat** zur **Datenkomprimierung** und **-archivierung**. Eine ZIP-Datei enthält einer oder mehrere Dateien, welche zur Verringerung der Dateigröße oder zum Abspeichern komprimiert wurden.

© 2013 IKARUS Security Software GmbH

© 2012 IKARUS Security Software GmbH. Alle Rechte vorbehalten.

Die in diesem Dokument enthaltenen Informationen stellen die Sichtweise der IKARUS Security Software GmbH zu den behandelten Themen zum Zeitpunkt der Veröffentlichung dar. Da die IKARUS Security Software GmbH auf sich ändernde Marktbedingungen reagieren muss, sind die in diesem Dokument enthaltenen Informationen nicht als Verpflichtung vonseiten der IKARUS Security Software GmbH zu verstehen, und IKARUS kann die Richtigkeit der in diesem Dokument enthalten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren.

Dieses Dokument dient lediglich Informationszwecken. DIE IKARUS Security Software GmbH ÜBERNIMMT IN DIESEM DOKUMENT KEINE AUSDRÜCKLICHEN ODER KONKLUDENTEN GARANTIEN.

Andere in diesem Dokument genannten Produkt- und Firmennamen sind möglicherweise Marken der jeweiligen Eigentümer.

IKARUS Security Software GmbH Blechturmgasse 11 in 1050 Wien Österreich